NATIONAL DEFENCE UNIVERSITY “CAROL I”

REGIONAL DEPARTMENT OF DEFENSE RESOURCES
MANAGEMENT STUDIES

INFORMATION SECURITY MANAGEMENT –
A NEW DECADE

Workshop unfolded during the postgraduate course in Information Security Management

13 - 14.06.2011, Brasov

Coordinator:

LTC Prof. eng. Daniel Sora, PhD

National Defense University „Carol I” Publishing House
BUCHAREST 2011

ISBN: 978-973-663-950-0

The contents of the papers is in the entire responsibility of the author(s), and does not necessarily reflect the opinion of the Scientific Board.

CONTENT

WIRELESS NETWORKS SECURITY

Lt. cdor Constantin CROITORU

INTRODUCTION

In today's business environment, controlling access to data is critical to long-term business survivability. Wireless is widely used because of the benefits it offers in its improved productivity, efficiency and cost effectiveness. The broad range of wireless technologies is no exception - such technologies allow for access to information outside an organization's normal perimeter.

Wireless signals are broadcast in an open and easily detected manner and will often travel well beyond the organization's physical security perimeter. As these technologies gain wider acceptance in the marketplace and increased adoption in the organization, these security risks require attention by the right people and at the right levels within your organization.

The widespread reliance on networking in business as well as the growth of the Internet and online services are strong testimonies to the benefits of shared data and resources. Wireless solutions advance these benefits by allowing users to access shared information, e-mail, and applications without the constraints of a wired connection. Further, wireless technology allows network managers to set up or augment networks without installing or moving wires. Almost all computing devices, including desktops, workstations, monitors, keyboards, notebooks, tablets, handhelds, and printers can be equipped to communicate wirelessly.

The availability of simple-to-use, more secure, wireless solutions have created the opportunity to reduce costs and improve performance. Business problems once thought of as "business as usual" are now being solved with wireless.

Wireless networks extend core networks, provides greater utilization of existing assets. Up-front expenses of the wireless network can be recovered in several cost saving areas; for example, dynamic environments requiring frequent moves and changes, adding network service to a new or temporary office, and adding connectivity to meeting rooms.

Wireless systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

I. WIRELESS NETWORKS TECHNOLOGIES

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders.

Wireless Networks. Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range:

- Wireless Wide Area Networks (WWAN)
- Wireless Local Area Networks (WLAN)
- Wireless Personal Area Networks (WPAN)

WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), and Global System for Mobile Communications (GSM). WLAN, representing wireless local area networks, includes 802.11, HiperLAN, and several others. WPAN represents wireless personal area network technologies such as Bluetooth and IR. All of these technologies are “tether-less” - they receive and transmit information using electromagnetic (EM) waves.

Although wireless LANs and wireless WANs may appear to be competing technologies, they are far more useful as complementary technologies. Used together, a user would have the best of both technologies, offering high-speed wireless access in a campus area, and access to all their data and applications with high-speed cellular access from anywhere with wireless WAN network coverage.

I.1. Wireless Local Area Network – WLAN

A wireless local area network (Wireless LAN) is a computer network that allows a user to connect without the need for a network cable. A laptop or PDA equipped with a wireless LAN card lets a user move around a building with their computer and stay connected to their network without needing to “plug in” with a cable. The most popular wireless LAN today is called an 802.11b network.

A WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter similar in function to a traditional Ethernet adapter. The coverage of a wireless access point can be up to 100 m (330 feet) indoors.

Wireless LANs are used in office buildings, on college campuses, or in houses, allowing multiple users shared access to one Internet connection. Some airports also plan to, or already offer wireless LAN access. Coffee shops, for example, are beginning to equip their shops with wireless LANs, which will allow laptop users to connect to the Internet.

WLANs provide wireless network communication over short distances using radio or infrared signals instead of traditional network cabling.

Network security remains an important issue for WLANs. Random wireless clients must usually be prohibited from joining the WLAN. Technologies like WEP raise the level of security on wireless networks to rival that of traditional wired networks.

I.2. Wireless Metropolitan Area Network - WMAN

Wireless Metropolitan Area Network (WMAN) is a computer network usually spanning a campus or a city, which typically connect a few local area networks using high speed backbone technologies. A MAN often provides efficient connections to a wide area network (WAN). There are three important features which discriminate MANs from LANs or WANs:

- The network size falls intermediate between LANs and WANs. A MAN typically covers an area of between 5 and 50 km range. Many MANs cover an area the size of a city, although in some cases MANs may be as small as a group of buildings.
- A MAN (like a WAN) is not generally owned by a single organization. The MAN, its communications links and equipment are generally owned by either a consortium of users or by a network service provider who sells the service to the users.
- A MAN often acts as a high speed network to allow sharing of regional resources. It is also frequently used to provide a shared connection to other networks using a link to a WAN.

This network enables you to access the Internet via a wireless wide area network (WWAN) access card and a PDA or laptop.

These networks provide a very fast data speed compared with the data rates of mobile telecommunications technology, and their range is also extensive. Cellular and mobile networks based on CDMA and GSM are good examples of WWAN. The WMAN technology uses the 802.16a standard that will provide broadband wireless connectivity to Fixed, Portable and Nomadic devices.

I.3. Wireless Wide Area Network – WWAN

A wireless wide area network (Wireless WAN) covers a much more extensive area than wireless LANs. Coverage is generally offered on a nationwide level with wireless network infrastructure provided by a wireless service carrier (for a monthly usage fee, similar to a cellular phone subscription).

While wireless LANs are used to allow network users to be mobile within a small fixed area, wireless WANs are used to give Internet connectivity over a much broader coverage area, for mobile users such as business travelers or field service technicians. Wireless WANs allow users to have access to the Internet, e-mail, and corporate applications and information even while away from their office.

Wireless WANs use cellular networks for data transmission and examples of the cellular systems that are used are: CDMA, GSM, GPRS and CDPD. A portable computer with a wireless WAN modem connects to a base station on the wireless networks via radio waves. The radio tower then carries the signal to a mobile switching center, where the data is passed on to the appropriate network. Using the wireless service provider’s connection to the Internet, data communications are established to an organization’s existing network.

Wireless WANs use existing cellular telephone networks, so there is also the option of making voice calls over a wireless WAN. Both cellular telephones and wireless WAN PC Cards have the ability to make voice calls as well as pass data traffic on wireless WAN networks.

A wired analogy of these complimentary technologies would be as follows: a user would plug their laptop (with built in network adapter) into a wired LAN connection while they are in the office. This gives them high-speed access to their e-mail, applications, data and the web. When they leave the office and work from home, or on the road at their hotel, they would use their dial up modem to have remote access to their e-mail, applications, and the web.

In the wireless example, the same user has a laptop with built-in wireless LAN access. This wireless LAN access is used for high-speed access to applications while in the office. Once out of the office, traveling to a local customer site, completing a work order in the field, or accessing e-mail from a hotel or airport, there is no longer any access to an 802.11 network. The wireless WAN card is now used to access a cellular provider’s network and obtain secure, remote access to e-mail, applications and the web.

Since many computers are now coming with wireless LAN devices built in, having a wireless WAN PC Card inserted into the computer would ensure that users can have high-speed wireless access where it is available, but still be able to access their important data with their wireless WAN card wherever there is cellular network coverage.

The following table summarizes the main differences between wireless LAN and Wireless WAN.

	Wireless LAN	Wireless WAN
Coverage	Office buildings or Campus with some public hotspots	Available wherever there is cellular network coverage; nationwide and global
Troughput speeds	1-5 Mb/s (however the underlying internet conection may yield a slower conection)	30-50 kb/s GPRS 40-70 kb/s CDMA2000 1x
Security	Security flaws	Secure encryption and authentication
Airtime charges	Airtime charges exist for most Hot spots acces. No airtime charges for office or home users (although ISP monthly service fee still exists)	Monthly subscription from wireless network provider.
Uses	Accessing a shared network within a building or across a campus	Remote access to corporate network for e-mail and applications. Web and internet access
Voice	No	Yes
Wired analogy	Ethernet Network	Remote modem access
Advantages	High speed. No airtime charges to set up networks (hardware costs and broadband internet connection fee still apply).	Ubiquitous coverage Secure network Access your data from anywhere
Disadvantages	Localized coverage only Security problems	Data rates faster than dial up, but not wireless LAN speeds yet.

II.WIRELESS STANDARDS USED IN WIRELESS NETWORKS

Wireless LANs based on the IEEE 802.11 or Wi-Fi standards have been a resounding success, and now the focus in wireless is shifting to the wide area. While Wi-Fi has virtually obliterated all other contenders in the local area, the wide area market is still up for grabs.

The cellular carriers got into the market first with their 2.5G/3G data services, but their offerings are positioned as an add-on to what is essentially a voice service. Sales have been lackluster to say the least. The real challenge to the cellular data services will come from the two emerging data-oriented technologies, WiMax and Mobile-Fi. With chip-level components due for shipment in the last quarter of 2004, WiMax will be the next to debut.

WiMax, short for Worldwide Interoperability for Microwave Access, is defined in IEEE 802.16 standards, and is being promoted by the WiMax Forum. The Forum looks to develop interoperability test suites to insure a multi-vendor solution that will result in lower cost products based on open standards. Internationally, a European Telecommunications Standards Institute (ETSI) initiative called HIPERMAN addresses the same area as WiMax/802.16 and shares some of the same technology.

With increased market recognition for WiMax, it is now regularly compared with Wi-Fi. While the two do indeed share some fundamental technical characteristics, they are approaching the wireless space from completely different perspectives. Further, different design approaches will make it unlikely that the two will actually compete except by coincidence. The purpose of this paper is to provide a technical and market comparison of the Wi-Fi and WiMax technologies highlighting their similarities and fundamental differences, and to identify the applications each will address in the coming years.

II.1. 802.11 – Wi-Fi (Wireless Fidelity)

Wi-Fi is a trademark of the Wi-Fi Alliance that may be used with certified products that belong to a class of wireless local area network (WLAN) devices based on the IEEE 802.11 standards. Because of the close relationship with its underlying standard, the term Wi-Fi is often used as a synonym for IEEE 802.11 technology.

A Wi-Fi enabled device such as a personal computer, video game console, mobile phone, MP3 player or personal digital assistant can connect to the Internet when within range of a wireless network connected to the Internet. The coverage of one or more interconnected access points — called a hotspot — can comprise an area as small as a few rooms or as large as many square miles covered by a group of access points with overlapping coverage.

IEEE 802.11 is a set of standards carrying out wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802).

The 802.11 family includes over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by 802.11g and 802.11n. Security was originally purposefully weak due to export requirements of some governments, and was later enhanced via the 802.11i amendment after governmental and legislative changes. 802.11n is a new multi-streaming modulation technique. Other standards in the family (c–f, h, j) are service amendments and extensions or corrections to the previous specifications.

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the US Federal Communications Commission Rules and Regulations. Because of this choice of frequency band, 802.11b and equipment may occasionally suffer interference from microwave ovens, cordless telephones and Bluetooth devices. Both 802.11 and Bluetooth control their interference and susceptibility to interference by using spread spectrum modulation. Bluetooth uses a frequency hopping spread spectrum signaling method (FHSS), while 802.11b and 802.11g use the direct sequence spread spectrum signaling (DSSS) and orthogonal frequency division multiplexing (OFDM) methods, respectively. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 19 non-overlapping channels rather than the 3 offered in the 2.4 GHz ISM frequency band. Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment.

The used segment of the radio frequency spectrum varies between countries. In the US, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations. Frequencies used by channels one through six (802.11b) fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under Part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption.

II.2. 802.16 – WiMAX (Worldwide Interoperability for Microwave Access)

WiMAX (Worldwide Interoperability for Microwave Access) is designed to deliver next-generation, high-speed mobile voice and data services and wireless “last-mile” backhaul connections that could potentially displace a great deal of existing radio air network (RAN) infrastructure. For network providers, this will enable an expansive array of multimedia and real-time subscriber services that go well beyond current 2.5/3G applications, including mobile streaming media services, mobile TV, Unified Communications, and Voice over IP (VoIP), which, for the first time, becomes practical and viable on a metro-wide scale through WiMAX.

Network service providers can’t take full advantage of mobile voice and multimedia over IP unless there is the potential to manage Quality of Service (QoS). With this in mind, five distinct classes of service quality have been built into WiMAX, allowing a more robust and resilient connection for users who require time-sensitive applications and service level agreements (SLAs).

WiMAX can offer a large wireless access network footprint to subscribers (similar to data-enabled cellular services such as UMTS/CDMA), while at the same time providing higher throughputs that are similar to WLAN networks. With its large footprint, high access speeds, built-in QoS and SLA capabilities, WiMAX is an ideal access network for next-generation converged voice and data services and streaming wireless multimedia.

The technology provides up to 10 Mbps broadband speed without the need for cables. The technology is based on the IEEE 802.16 standard (also called Broadband Wireless Access).

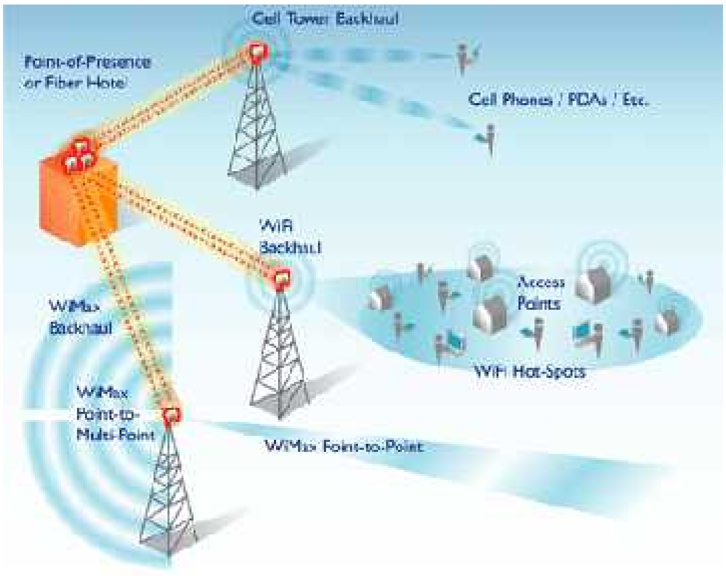
The terms "WiMAX", "mobile WiMAX", "802.16d" and "802.16e" are frequently used incorrectly. Correct definitions are the following:

- 802.16-2004 is often called 802.16d, since that was the working party that developed the standard. It is also frequently referred to as "fixed WiMAX" since it has no support for mobility.
- 802.16e-2005 is an amendment to 802.16-2004 and is often referred to in shortened form as 802.16e. It introduced support for mobility, among other things and is therefore also known as "mobile WiMAX".

WiMAX is a possible replacement candidate for cellular phone technologies such as GSM and CDMA, or can be used as an overlay to increase capacity. It has also been considered as a wireless backhaul technology for 2G, 3G and 4G networks in both developed and poor nations.

As a standard intended to satisfy needs of next-generation data networks (4G), 802.16e is distinguished by its dynamic burst algorithm modulation adaptive to the physical environment the RF signal travels through. Modulation is chosen to be spectroscopically more efficient (more bits per OFDM/SOFDMA symbol). That is, when the bursts have a high signal strength and a carrier to noise plus interference ratio (CINR), they can be more easily decoded using digital signal processing (DSP). In contrast, operating in less favorable environments for RF communication, the system automatically steps down to a more robust mode (burst profile) which means fewer bits per OFDM/SOFDMA symbol; with the advantage that power per bit is higher and therefore simpler accurate signal processing can be performed.

A commonly-held misconception is that WiMAX will deliver 70 Mbps over 50 kilometers (30 miles). In reality, WiMAX can either operate at higher bitrates or over longer distances but not both: operating at the maximum range of 50 km increases bit error rate and thus results in a much lower bitrate. Conversely, reducing the range (to under 1 km) allows a device to



operate at higher bitrates. There are no known examples of WiMAX services being delivered at bit rates over around 40 Mbps.

Like most wireless systems, available bandwidth is shared between users in a given radio sector, so performance could deteriorate in the case of many active users in a single sector. In practice, most users will have a range of 2-3 Mbps services and additional radio cards will be added to the base station to increase the number of users that may be served as required.

Future development. The IEEE 802.16m standard is the core technology for the proposed Mobile WiMAX Release 2, which enables more efficient, faster, and more converged data communications. The IEEE 802.16m standard has been submitted to the ITU for IMT-Advanced standardization. IEEE 802.16m is one of the major candidates for IMT-Advanced technologies by ITU. Among many enhancements, IEEE 802.16m systems can provide four times faster data speed than the current Mobile WiMAX Release 1 based on IEEE 802.16e technology.

Mobile WiMAX Release 2 will provide strong backward compatibility with Release 1 solutions. It will allow current Mobile WiMAX operators to migrate their Release 1 solutions to Release 2 by upgrading channel cards or software of their systems. Also, the subscribers who use currently available Mobile WiMAX devices can communicate with new Mobile WiMAX Release 2 systems without difficulty.

It is anticipated that in a practical deployment, using 4X2 MIMO in the urban microcell scenario with only a single 20-MHz TDD channel available system wide, the 802.16m system can support both 120 Mbps downlink and 60 Mbps uplink per site simultaneously. It is expected that the WiMAX Release 2 will be available commercially in the 2011-2012 timeframe.

The goal for the long-term evolution of WiMAX is to achieve 100 Mbps mobile and 1 Gbps fixed-nomadic bandwidth as set by ITU for 4G NGMN (Next Generation Mobile Network).

Comparison with Wi-Fi. Comparisons and confusion between WiMAX and Wi-Fi are frequent because both are related to wireless connectivity and Internet access:

- WiMAX is a long range system, covering many kilometers, that uses licensed or unlicensed spectrum to deliver a point-to-point connection to the Internet;
- Different 802.16 standards provide different types of access, from portable (similar to a cordless phone) to fixed (an alternative to wired access, where the end user's wireless termination point is fixed in location);
- Wi-Fi uses unlicensed spectrum to provide access to a network;
- Wi-Fi is more popular in end user devices;
- WiMAX and Wi-Fi have quite different quality of service (QoS) mechanisms:

  - WiMAX uses a QoS mechanism based on connections between the base station and the user device. Each connection is based on specific scheduling algorithms.
  - Wi-Fi has a QoS mechanism similar to fixed Ethernet, where packets can receive different priorities based on their tags. For example VoIP traffic may be given priority over web browsing.
- Wi-Fi runs on the Media Access Control's CSMA/CA protocol, which is connectionless and contention based, whereas WiMAX runs a connection-oriented MAC;
- Both 802.11 and 802.16 define Peer-to-Peer (P2P) and ad hoc networks, where an end user communicates to users or servers on another Local Area Network (LAN) using its access point or base station.

II.3. 3G and 4G

International Mobile Telecommunications-2000 (IMT-2000), better known as **3G** or **3rd Generation**, is a family of standards for mobile telecommunications defined by the International Telecommunication Union, which includes GSM EDGE, UMTS, and CDMA2000 as well as DECT and WiMAX. Services include wide-area wireless voice telephone, video calls, and wireless data, all in a mobile environment. Compared to 2G and 2.5G services, 3G allows simultaneous use of speech and data services and higher data rates (up to 14.0 Mbps on the downlink and 5.8 Mbps on the uplink with HSPA+). Thus, 3G networks enable network operators to offer users a wider range of more advanced services while achieving greater network capacity through improved spectral efficiency.

Security. 3G networks offer a greater degree of security than 2G predecessors. By allowing the UE (User Equipment) to authenticate the network it is attaching to, the user can be sure the network is the intended one and not an impersonator. 3G networks use the KASUMI block crypto instead of the older A5/1 stream cipher. However, a number of serious weaknesses in the KASUMI cipher have been identified.

In addition to the 3G network infrastructure security, end-to-end security is offered when application frameworks such as IMS are accessed, although this is not strictly a 3G property.

Applications. The bandwidth and location information available to 3G devices gives rise to applications not previously available to mobile phone users. Some of the applications are:

- Mobile TV - a provider redirects a TV channel directly to the subscriber's phone where it can be watched.
- Video on demand - a provider sends a movie to the subscriber's phone.

- Video conferencing - subscribers can see as well as talk to each other.
- Tele-medicine - a medical provider monitors or provides advice to the potentially isolated subscriber.
- Location-based services - a provider sends localized weather or traffic conditions to the phone, or the phone allows the subscriber to find nearby businesses or friends.

2G networks were built mainly for voice services and slow data transmission.

From 2G to 2.5G. The first major step in the evolution to 3G occurred with the introduction of General Packet Radio Service (GPRS). So the cellular services combined with GPRS became "*2.5G*".

GPRS could provide data rates from 56 kbps up to 114 kbps. It can be used for services such as Wireless Application Protocol (WAP) access, Multimedia Messaging Service (MMS), and for Internet communication services such as email and World Wide Web access. GPRS data transfer is typically charged per megabyte of traffic transferred, while data communication via traditional circuit switching is billed per minute of connection time, independent of whether the user actually is utilizing the capacity or is in an idle state.

From 2.5G to 2.75G (EDGE). GPRS networks evolved to EDGE networks with the introduction of 8PSK encoding. Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), or IMT Single Carrier (IMT-SC) is a backward-compatible digital mobile phone technology that allows improved data transmission rates, as an extension on top of standard GSM. EDGE was deployed on GSM networks beginning in 2003 - initially by Cingular (now AT&T) in the United States.

EDGE is standardized by 3GPP as part of the GSM family, and it is an upgrade that provides a potential three-fold increase in capacity of GSM/GPRS networks. The specification achieves higher data-rates by switching to more sophisticated methods of coding (8PSK), within existing GSM timeslots.

Evolution towards 4G. Both 3GPP and 3GPP2 are currently working on further extensions to 3G standards, named Long Term Evolution and Ultra Mobile Broadband, respectively. Being based on an all-IP network infrastructure and using advanced wireless technologies such as MIMO, these specifications already display features characteristic for IMT-Advanced (4G), the successor of 3G. However, falling short of the bandwidth requirements for 4G (which is 1 Gbps for stationary and 100 Mbps for mobile operation), these standards are classified as 3.9G or Pre-4G.

3GPP plans to meet the 4G goals with LTE Advanced, whereas Qualcomm has halted development of UMB in favour of the LTE family.

4G refers to the fourth generation of cellular wireless standards. It is a successor to 3G and 2G standards, with the aim to provide a wide range of data rates up to ultra-broadband (gigabit-speed) Internet access to mobile as well as stationary users. Although 4G is a broad term that has had several different and more vague definitions, this article uses 4G to refer to IMT Advanced (International Mobile Telecommunications Advanced), as defined by ITU-R.

A 4G cellular system must have target peak data rates of up to approximately 100 Mbps for high mobility such as mobile access and up to approximately 1 Gbps for low mobility such as nomadic/local wireless access, according to the ITU requirements. Scalable bandwidths up to at least 40 MHz should be provided. A 4G system is expected to provide a comprehensive and secure all-IP based solution where facilities such as IP telephony, ultra-broadband Internet access, gaming services and HDTV streamed multimedia may be provided to users.

4G is being developed to accommodate the QoS and rate requirements set by further development of existing 3G applications like wireless broadband access, Multimedia Messaging Service (MMS), video chat, mobile TV, but also new services like HDTV content, minimal services like voice and data, and other services that utilize bandwidth. It may be allowed roaming with wireless local area networks, and be combined with digital video broadcasting systems.

The 4G working group has defined the following as objectives of the 4G wireless communication standard:

- Flexible channel bandwidth, between 5 and 20 MHz, optionally up to 40 MHz.
- A nominal data rate of 100 Mbps while the client physically moves at high speeds relative to the station, and 1 Gbps while client and station are in relatively fixed positions as defined by the ITU-R.
- A data rate of at least 100 Mbps between any two points in the world.
- Peak link spectral efficiency of 15 bps/Hz in the downlink, and 6.75 bps/Hz in the uplink (meaning that 1000 Mbps in the downlink should be possible over less than 67 MHz bandwidth).
- System spectral efficiency of up to 3 bps/Hz/cell in the downlink and 2.25 bps/Hz/cell for indoor usage.
- Smooth handoff across heterogeneous networks.
- Seamless connectivity and global roaming across multiple networks.
- High quality of service for next generation multimedia support (real time audio, high speed data, HDTV video content, mobile TV, etc.).
- Interoperability with existing wireless standards.
- An all IP, packet switched network.

II.4. Comparison of Mobile Internet Access methods

Comparison of Mobile Internet Access methods						
Standard	Family	Primary Use	Radio Tech	Downlink (Mbps)	Uplink (Mbps)	Notes
LTE	UMTS/4GSM	General 4G	OFDMA/MIMO/SC-FDMA	360	80	LTE-Advanced update expected to offer peak rates of at least 1 Gbps fixed speeds and 100 Mbps to mobile users.
WiMAX	802.16e	Mobile Internet	MIMO-SOFDMA	144	35	WiMAX update IEEE 802.16m expected offer up to 1 Gbps fixed speeds.
Flash-OFDM	Flash-OFDM	Mobile Internet mobility up to	Flash-OFDM	5.3 10.6	1.8 3.6 5	Mobile range 18miles (30km) extended range 34 miles (55km)

		200 mph (350km/h)		15.9	.4	
HIPERMAN	HIPERMAN	Mobile Internet	OFDM	56.9	56.9	
Wi-Fi	802.11(11n)	Mobile Internet	OFDM/MIMO	288.9 (Supports 600Mbps @ 40MHz channel width)		Antenna, RF front end enhancements and minor protocol timer tweaks have helped deploy long range P2P networks compromising on radial coverage, throughput and/or spectra efficiency (310km & 382km).
iBurst	802.20	Mobile Internet	HC-SDMA/TDD/MIMO	95	36	Cell Radius: 3–12 km Speed: 250kmph Spectral Efficiency: 13 bits/s/Hz/cell Spectrum Reuse Factor: "1"
EDGE Evolution	GSM	Mobile Internet	TDMA/FDD	1.9	0.9	3GPP Release 7
UMTS W-CDMA HSDPA	UMTS/3G	General 3G	CDMA/FDD	0.384 1	0.384 5	HSDPA widely deployed. Typical downlink rates today 2 Mbps, ~200 kbps uplink; HSPA+ downlink up to 42 Mbps.

A+ HSUPA HSPA+	SM		CDMA/FDD D/MIMO	4.4 42	.76 11.5	
UMTS-TDD	UMTS/3GSM	Mobile Internet	CDMA/TDD	16	16	Reported speeds according to IPWireless using 16QAM modulation similar to HSDPA+HSUPA
1xRTT	CDMA2000	Mobile phone	CDMA	0.144	0.144	Succeeded by EV-DO
EV-DO 1x Rev. 0 EV-DO 1x Rev. A EV-DO Rev. B	CDMA2000	Mobile Internet	CDMA/FDD	2.45 3.1 4.9xN	0.15 1.8 1.8xN	Rev B note: N is the number of 1.25 MHz chunks of spectrum used. Not yet deployed.

III. WIRELESS SECURITY: RISKS AND DEFENSES

Security is one of the most important features when using a wireless network. Security is one of the biggest strengths for cellular wireless networks (WWANs) and one of the biggest weaknesses in 802.11 networks (WLANs). 802.11b networks have several layers of security; however there are weaknesses in all of these security features. The first level of security is to have wireless LAN authentication done using the wireless adapter's hardware (MAC) address.

Security can be increased on wireless LANs by using shared key authentication. This shared key must be delivered through a secure method other than the 802.11 connection. In practice, this key is manually configured on the access point and client, which is not efficient on a large network with many users. This shared key authentication is not considered secure and is not recommended to ensure security.

Another weakness in an 802.11 network is the difficulty in restricting physical access to the network, because anyone within range of a wireless access point can send, receive, or intercept frames. WEP (Wired Equivalency Protocol) was designed to provide security equivalent to a wired network by encrypting the data sent between a wireless client and an access point.

However, key management is a significant problem with WEP. WEP keys must be distributed via a secure channel other than 802.11. The key is normally a text string that needs to be manually configured on the wireless access point and wireless clients, which is not practical to a large network. There is also no mechanism to change the WEP key regularly or periodically, so all wireless access points and clients use the same manually configured WEP. With several wireless clients sending large amounts of data, without changing the WEP key, it is possible to intercept data traffic and determine the WEP key. This would allow a hacker to intercept and decrypt the data traffic.

Another problem that has been reported with wireless LANs is that when the security features are turned on, there are problems with interoperability between wireless LAN modules from one vendor and wireless LAN access points from another vendor.

Wireless LANs were designed specifically to operate in the 2.4 GHz band, which is a globally allocated frequency for unlicensed operation. This means that there is no requirement to be a licensed operator to run a wireless LAN in this frequency. A wireless WAN however operates in tightly regulated frequency spectrums and all operators must be licensed to operate in this frequency. This implies much better data security and protection, since licensed operators have to follow government regulations for wireless access.

In contrast to the security weaknesses in 802.11 networks, cellular wireless WAN networks are extremely secure. These networks incorporate military technology and sophisticated encryption and authentication methods.

III.1. Types of Security

WEP (Wired Equivalent Privacy). Developed in the late 1990s, WEP is a basic protocol that is sometimes overlooked by wireless administrators because of its numerous vulnerabilities. The original implementations of WEP used 64-bit. By means of a Brute Force attack, 64-bit WEP can be broken in a matter of minutes, whereas the stronger 128-bit version will take hours. It's not the best line of defense against unauthorized intruders but better than nothing and mainly used by the average home user. One of the drawbacks of WEP is that since it uses a shared key, if someone leaves the company then the key will have to be changed on the access point and all client machines.

WEP2 (Wired Equivalent Privacy version 2). In 2004, the IEEE proposed an updated version of WEP; WEP2 to address its predecessor's shortcomings. Like WEP it relies on the RC4 algorithm but instead uses a 128-bit initialization vector making it stronger than the original version of WEP, but may still be susceptible to the same kind of attacks.

WPA (Wi-Fi Protected Access). WPA provides encryption via the Temporary Key Integrity Protocol (TKIP) using the RC4 algorithm. It is based on the 802.1X protocol and addresses the weaknesses of WEP by providing enhancements such as Per-Packet key construction and distribution, a message integrity code feature and a stronger IV (Initialization Vector). The downside of WPA is that unless the current hardware supports WPA by means of a firmware upgrade, you will most likely have to purchase new hardware to enjoy the benefits of this security method. The length of a WPA key is between 8 and 63 characters – the longer it is the more secure it is.

WPA2 (Wi-Fi Protected Access version 2). Based on the 802.11i standard, WPA2 was released in 2004 and uses a stronger method of encryption – AES (Advanced Encryption Standard). AES supports key sizes of 128 bits, 192 bits, and 256 bits. It is backward compatible with WPA and uses a fresh set of keys for every session, so essentially every packet that sent over the air is encrypted with a unique key. As did WPA, WPA2 offers two versions – Personal and Enterprise. Personal mode requires only an access point and uses a pre-shared key for authentication and Enterprise mode requires a RADIUS authentication server and uses EAP.

MAC Address Filtering. MAC Address Filtering is a means of controlling which network adapters have access to the access point. A list of MAC Addresses is entered into the access point and anyone whose MAC address on the wireless network adapter does not match an entry in the list will not be permitted entry. This is a pretty good means of security when also used with a packet encryption method. However, keep in mind that MAC addresses can be spoofed. This type of security is usually used as a means of authentication, in conjunction with something like WEP for encryption.

SSID (Service Set Identifier). An SSID, or Network Name, is a "secret" name given to a wireless network. By default, the SSID is a part of every packet that travels over the WLAN. Unless you know the SSID of a wireless network you cannot join it. Every network node must be configured with the same SSID of the access point that it wishes to connect, which becomes a bit of a headache for the network administrator.

VPN (Virtual Private Network) Link. Perhaps the most reliable form of security would be to setup a VPN connection over the wireless network. VPNs have for long been a trusted method of accessing the corporate network over the internet by forming a secure tunnel from the client to the server. Setting up a VPN may affect performance due to the amount of data encryption involved. The VPN option is preferred by many enterprise administrators because VPNs offer the best commercially available encryption. VPN software uses advanced encryption mechanisms (AES for example), which makes decrypting the traffic a very hard, if not impossible, task.

III.2. Risks/Vulnerabilities

In addition to all the vulnerabilities common to wired networks, wireless LANs introduce a new series of risks. The critical vulnerabilities are eavesdropping, illicit entry into the network and denial of service. Some users may perceive they are at risk from being exposed to radio wave energy, but there is no credible research supporting this thesis, and US FCC Part 15 certification requires that devices meet the government standard for exposure.

Eavesdropping. By their nature, wireless LANs radiate network traffic into space. Once that is done, it is impossible to control who can receive the signals. So, it must be assumed in any wireless LAN installation that the network traffic is subject to interception and eavesdropping by third parties. The obvious solution to this problem is to encrypt the data stream. The 802.11 standards provide for doing precisely that. Unfortunately, the implementation of this solution is less than perfect.

To provide security on wireless LANs, the 802.11b standard provides for wired equivalent privacy (WEP). There are several problems with the implementation of this approach. First, WEP is an option. It is not activated by default in shipped products, and it reduces raw throughput by as much as 50 percent. In such a situation, the network is broadcasting all network traffic in the clear for the benefit of all who can intercept it. That is hardly a secure mode of operation.

The WEP approach to cryptography sounds secure: WEP encrypts every packet with a different key. It uses a straightforward and predictable way of incrementing the vector from one packet to the next. Coupled with weak key management and a restricted key space, WEP is demonstrably insecure. The WEP password scheme also has been found to be flawed with the result that an intruder can gain access to some WEP-protected networks in as little as 30 seconds.

There are technologies that can be employed to provide cryptographic level confidentiality beyond what is offered by WEP. The researchers who "broke" WEP recommend treating all wireless networks as being outside the firewall and using higher-level protocols, such as SSH or IPSec, to provide security.

The goal of WEP was to provide a level of security commensurate with that found on wired LANs. Wired networks are not generally very secure unless protected by measures beyond those provided by the network protocols. Many have experienced connecting a computer to a wired LAN and being able suddenly to access resources to which they had no right. This is a common problem, usually controlled by limiting which computers may physically connect to the LAN. However, in the wireless domain, it is more difficult to limit who can connect to the LAN, so WEP - despite its shortcomings - is an important tool in the overall management of network security.

Illicit Entry. The very nature of the wireless protocols is to make the network user friendly by facilitating connection to an access point - and thus the entire network - as the user moves about. That is to say, the system has weak authentication.

Wireless network equipment is generally set so the network name is a default name for public access and all network interface cards that conform to the standard of the network (e.g., 802.11b) can readily connect to the system. Few network administrators bother to change the level of access to something more restrictive than the default. The wireless access point advertises its presence and its network name, and when a wireless client senses the access point, the client attempts to connect to the network. Unless the ability to connect is somehow restricted, the connection attempt will succeed, and another user will have been added to those already supported. As wireless LANs primarily serve to extend wired networks, the view this newcomer has of the network may be quite extensive, and the resources available may include many not intended for casual visitors. With a wireless LAN, one only has to be in the vicinity. As it happens, the vicinity may be rather large.

Depending on the structural elements in the path, a wireless LAN signal may be usable for distances of approximately 500 meters. While this is helpful from a coverage standpoint, it is not helpful from a security standpoint. Using directional antennae, one can detect wireless network signals at distances up to eight miles (12.8 kilometers) from the network node. In such a situation, someone can connect to a network from outside the perimeter of a place of business and probably without the organization's knowledge.

Large networks that cater to itinerant users are more or less forced to accept the poor authentication provided by WEP. It would not do if one had to register in advance to use a network in a public airport space, for instance. However, smaller networks have an option that can help. It is possible to restrict access to the network to those network nodes whose media access control (MAC) addresses are known in advance by the access point. For small wireless networks with a stable user population, this is an attractive option.

Denial of Service. A denial-of-service (DoS) attack is one wherein the attacker attempts to render the target network unable to serve its legitimate users. In the wired domain, many have become accustomed to protocol-based attacks, such as the "Ping of Death," which seek to overwhelm the target network with traffic forcing the network servers to crash. This type of attack also is effective against wireless networks.

In addition to protocol-based DoS attacks, wireless networks are vulnerable to a denial-of-service attack that is not viable against their wired brethren. Because their signals must travel through the public airwaves rather than in protected cables, wireless networks are extremely vulnerable to radio interference, either deliberate or accidental. Accidental interference occurs all too often owing to the shared nature of the bands in which these networks operate. It is very common for a wireless network, or a portion of it, to become unusable when a cordless telephone is operating in the same band and in physical proximity to the wireless node. It also is common for one wireless network to interfere with another nearby network, often making both useless.

III.3. Defense in Depth

In deploying a wireless LAN, the same importance must be stressed in terms of security as when deploying a wired LAN. Security must be looked at several aspects like in the policy and the three A's of Security - Access control, Authentication and Auditing. Defense in depth, in particular, defines several layers with each layer having its own security mechanisms and controls. The layers are the perimeter defense, network, host, application and information.

Authentication will look at the perimeter defense and the network layer. This is basically looking at how users get authenticated and what defense strategies are applied at the perimeter. Access control meanwhile will define who can have access to the wireless network and how to control and monitor them. It will also look at the access control at the host level and application by implementing host based firewall for example. As to protect the information, security policies and procedures need to be defined and enforced while auditing the wireless network with relevant tools will strengthen all the layers defined earlier.

Security Policy and Procedure. As we know, all technologies will have their own advantages, disadvantages and limitations that will make the technologies useful to the users. Nonetheless, technology alone will not be able to be utilized to its most potential without the intervention of human factor, like the policies and procedures. Policies and procedures will become the guidelines for technology to be properly used and to get the most out of it. Hence, it is vital that any deployment of wireless LAN is preceded by a wireless security policy. Having a security policy that defines the right procedures for implementing wireless networks will help reduce the risk of wireless network being breached. Policy and procedures can help enforced standard rules sets required in a deployment of wireless network.

Hence, it is recommended to implement the following security controls in order to maximize the 802.11b network by following certain best practices:

- Disable broadcast of the 32-bit plain text Service Set Identifier (SSID). This way, only clients with the known correct SSID can associate with the access point.
- More sophisticated attackers will counter a lack of broadcast SSID by analyzing the authentication frames with an 802.11 scanner to obtain the plain text SSID. To limit the effect of passive attacks, if possible, only broadcast beacon packets at higher bandwidth and reduce the frequency of beacon packets to inhibit such methods.
- Set non-standard SSIDs. Do not use the company name, address or any other easy to guess information about the organization.
- Do not choose SSIDs that could be attractive to attackers. Follow strong password generation methods to create SSIDs that are difficult to guess.
- Always enable 40-bit or 128-bit WEP encryption. Although there are numbers of WEP shortcomings, it will be a barrier to casual attack.
- Choose strong encryption keys on all wireless devices and change shared keys regularly. Encryption key changes make it harder for attackers to obtain and maintain a foothold on the network.
- Change all default vendor passwords.
- Administer the wireless devices using secure protocols like SSH or HTTPS, instead of telnet and HTTP.

Authentication. Authentication is always the best possible security measures in any systems. In 802.11, it specifies two major approaches which are open system authentication and shared key authentication.

Open system authentication is the default authentication method for 802.11. In open system authentication, the access point accepts anyone who requests authentication without verifying its identity. It works by exchanging only two management frames between the mobile station and access points.

Shared key authentication makes use of Wired Equivalent Privacy (WEP) and requires a shared key to be distributed to stations before attempting authentication. As with open system authentication, it works by exchanging management frames except with shared key authentication, it uses four frames instead of two.

There is another mechanism used by vendors to provide security with the use of access control lists based on the Ethernet MAC address of the client. Each access points can limit the clients of the network to those using a listed MAC he addresses. If a client's MAC address is listed, then they are permitted access to the network or else they will be rejected. Moreover, it is important to note one security problem with the MAC access control list. This mechanism only authenticates the machine with the right MAC address but not the users.

Access Control. The nature of wireless networks can be treated as an external network to the enterprise LAN. As such, any security measure taken to secure the network from Internet access, for example, can also be applied to the wireless network, as well.

One of the measures that can be applied to secure wireless LAN is by implementing a wireless firewall gateway. Wireless firewall is actually a wired firewall that bridges the wireless network and the wired network.

Packet filtering can also be applied at the firewall to allow only selected lied protocols or hosts into the network.

In addition to having a firewall, an intrusion detection system must also be installed between the wireless network and the wired network. Intrusion detection system or IDS should be able to add more security to the network by sniffing, the wireless traffics and alerting the administrators on suspected malicious traffics through defined signatures. This vigilance monitoring will provide administrators preventive and also response security measure as certain malicious traffics could be blocked before doing some damage to the network.

Furthermore, we can also deploy DHCP for issuing and maintaining IP addresses of wireless networks' clients. DHCP also allows to group users into IP address range that is based on the requirement and defined in the firewall. This kind of arrangement will allow legitimate users to get access to the network and restrict other unnecessary access.

At the host level, it is recommended to have some kind of filtering mechanism like the personal firewall. This is to provide security access control and measure at the application and host layer.

Auditing. Auditing the network is supposed to be the top priority for all network administrators. By auditing the network, we are actually looking at the vulnerabilities that are available inside the wireless networks. By finding and knowing what type of vulnerabilities existed in the network, it will prepare the administrators to put necessary measures to overcome or prevent any kind of threats that resulted from the vulnerabilities.

CONCLUSIONS

Wireless LANs are very valuable in today's mobile society. They have proliferated over the past few years, and although the market has not quite reached its maturity level due to refinements to some of the hardware and software, it is no longer a secret to the public at large. Anyone who does not personally have a wireless LAN knows someone who does, uses one at work, has heard of the technology or is unknowingly affected by the technology each day of their lives. Although wireless LANs for both small office/home office and the enterprise have some security vulnerabilities, if care is taken to implement the following safeguards the vulnerabilities will be greatly minimized or removed allowing the LAN to be used safely:

- inform and train users
- configure the access points
- monitor the LANs
- use strong encryption
- implement 802.1X with authentication, authorization and accounting (AAA)
- deploy an EAP method

To compliment the measures above, there should also be:

- a system of checks and balances in place, for example, have a second IT staff member double checked the access point configuration.
- a plan to consistently demand better products from manufacturers
- an effort to stay abreast of the latest in developing technology

With newer technology that promises greater built-in or add-on security measures, wireless LANs will attract greater, more sophisticated hacker attacks - another chapter in the continuing saga of security versus hacker. We know that hackers will never go away, so we bear the burden to provide the best “locks” we can to protect our LANs. Finally, whatever the outcome, wireless LANs will survive and are here to stay even if the technology has a new look and, or feel in coming years.

REFERENCES

1. Earle A. - *Wireless Security Handbook*, Auerbach Publications, New York, 2006
2. Finneran M. - *WiMax versus Wi-Fi, a Comparison of Technologies*, 2005
3. PhD. Zota R., - New *Broadband Wireless Technologies – WiMax*, in Economic Informatics Magazine, Bucharest, 2006
4. John J. Laskar, - *Concept of Secure Wireless Metropolitan Area Network (SWMAN) in a Mobile Computing Environment*, Mitretek Systems
5. Vladimirov A., Gavrilenko K. V. - *Wi-Foo*, Addison Wesley, 2004
6. *MOTOROLA WI4 WiMAX*, Solutions Guide

WEBLINKS

7. http://en.wikipedia.org/wiki/WLAN, http://en.wikipedia.org/wiki/WWAN
8. http://en.wikipedia.org/wiki/WWAN
9. www.about.com
10. "*Top 5 Wireless Tools*", http://sectools.org/wireless.html, 2006
11. http://en.wikipedia.org/wiki/Wi-Fi
12. http://en.wikipedia.org/wiki/WiMAX
13. http://en.wikipedia.org/wiki/3G, http://en.wikipedia.org/wiki/4G
14. http://en.wikipedia.org/wiki/4G
15. www.securityoverview.com
16. http://www.army-technology.com/features/feature41023/
17. http://www.radio-electronics.com/info/wireless/index.php
18. http://www.wirelessoverview.net/wireless-security?start=9
19. http://www.wifinotes.com/
20. http://www.javvin.com/wirelessmap.html
21. http://defense-update.com/features/du-1-05/c4-data.htm
22. http://netsecurity.about.com/cs/hackertools/a/aafreewifi.htm
23. http://docs.lucidinteractive.ca/index.php/Cracking_WEP_and_WPA_Wireless

CRYPTOGRAPHY IN DATA SECURITY

1st LT Eduard Eusebiu EMANDII

INTRODUCTION

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact we have made our position unassailable.[1]

Information has always meant power, so the biggest problem of our technological age is protecting the information. Nowadays, it is more obvious that computers and cryptography are in a tight relation because with the development of computers we need new and more complex cryptographic techniques.

But what cryptography means? The most suitable definition for cryptography is that it provides secured information between two or more correspondents in the presence of an adversary. So the main objective in using cryptography is to secure information transmitted through an insecure channel. In modern times, cryptography is considered a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering.

Cryptography was widely used by military and governments to facilitate secret communication. Over the years, mathematicians and computer scientists have developed a series of increasingly complex algorithms designed to ensure data security. While cryptographers spent time developing strong encryption algorithms, hackers and governments alike devoted significant resources to undermining those cryptographic algorithms. This led to an "arms race" in cryptography and resulted in the development of the extremely sophisticated algorithms in use today. Nowadays, cryptography is frequently used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, stored data on servers which all depend on cryptography. For example, many people are under the mistaken impression that email is point to point communication protocol, but it is not. Many servers are envolved, and each of them can mess with your messages, unless you protect them.

Data security refers at two aspects, the first is the protection of data stored on computers, laptops, servers or back-ups servers and the second refers to network security and information transmitted through an insecure channel.

[1] Sun Tzu – *The art of War*

I. BASIC ELEMENTS IN CRYPTOGRAPHY

I.1. Terminology

The word "cryptography" is derived from the Greek words *kryptos*, meaning hidden, and *graphien*, meaning to write. Historians believe Egyptian hieroglyphics, which began about 1900 B.C.E., to be an early instance of encipherment. The key that unlocked the hieroglyphic secrets was the Rosetta Stone, discovered in 1799 in lower Egypt and now located in the British Museum in London.

Cryptography is the science of using mathematics to encrypt and decrypt data and it is practiced by *cryptographers*. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

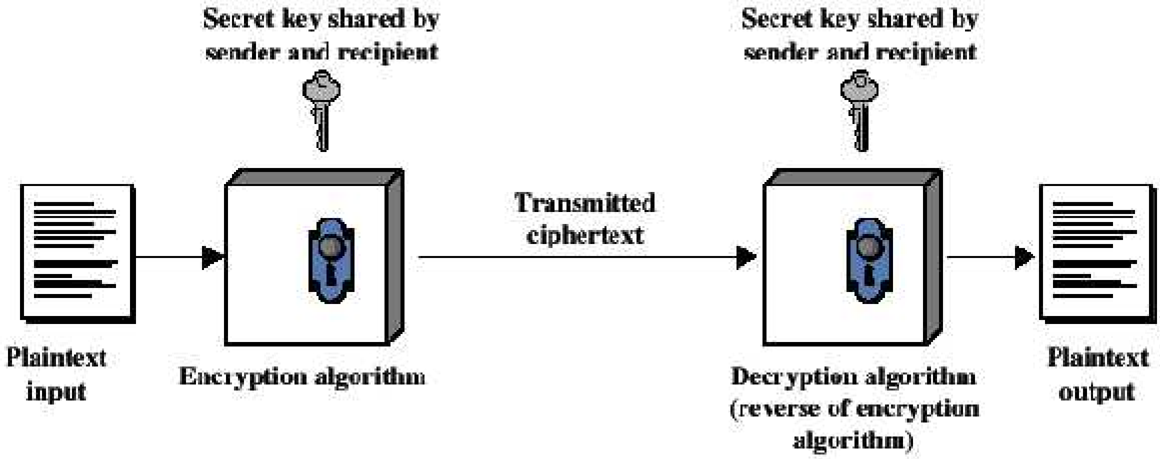

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 1 – Encryption/decryption scheme

A message is *plaintext* (sometimes called cleartext). The process of disguising a message in such a way as to hide its meaning is *encryption.* An encrypted message is *ciphertext.* The process of turning ciphertext back into plaintext is *decryption*. *Cryptanalysts* are practitioners of *cryptanalysis*, the art and science of breaking ciphertext; that is, seeing through the disguise. A *cryptosystem* is an algorithm, plus all possible plaintexts, ciphertexts, and keys. The branch of mathematics encompassing both cryptography and cryptanalysis is *cryptology* and its practitioners are *cryptologists*.

I.2. General principles

Security practitioners utilize cryptographic systems to meet four fundamental goals: confidentiality, integrity, authentication, and nonrepudiation.

Confidentiality ensures that a message remains private during transmission between two or more correspondents. This is perhaps the most important goal of cryptosystems—the facilitation of secret communications between individuals and groups. Two main types of cryptosystems enforce confidentiality. Symmetric key cryptosystems use a shared secret key available to all users of the cryptosystem. Public key cryptosystems utilize individual combinations of public and private keys for each user of the system.

Integrity ensures that a message is not altered on his way from a correspondent to another. If integrity mechanisms are in place, the recipient of a message can be certain that the message received is identical to the message that was sent. This protects against all forms of alteration, which can be intentional alteration by a third party attempting to insert false information or unintentional alteration by faults in the transmission process. Message integrity is enforced through the use of digitally signed message digests created upon transmission of a message. The recipient of the message must to verify if the message's digest and signature are valid, ensuring that the message was not altered in transit. Integrity can be enforced by both public and secret key cryptosystems.

Authentication verifies the claimed identity of system users and is very important for functionality of cryptosystems. For example, someone could use the public key and send an encrypted message just to misleading someone. That's way we must be sure that the sender of the message is who claimed to be.

Nonrepudiation ensures that the sender has strong evidence that the receiver has received the message, and the receiver has strong evidence of the sender identity, strong enough such that the sender cannot deny that it has sent the message and the receiver cannot deny that it has received the message.

Also, all cryptographic algorithms rely upon keys to maintain their security. For the most part, a key is nothing more than a number. It's usually a very large binary number. Every algorithm has a specific *key space*. The key space is the range of values that are valid for use as a key for a specific algorithm. A key space is defined by its bit size. Bit size is nothing more than the number of binary bits or digits in the key. The key space is the range between the key that has all 0s and the key that has all 1s. Or to state it another way, the key space is the range of numbers from 0 to 2^n, where n is the bit size of the key. So, a 128-bit key can have a value from 0 to 2^{128} (which is roughly $3.40282367 * 10^{38}$). Even though a key is just a number, it is a very important one, because if the algorithm is known, then all the security you gain from cryptography rests on your ability to keep the keys used private.

Encryption can be used to protect data "at rest", such as data files from computers and storage media (USB flash drives). In recent years there have been numerous reports of exposures of confidential data such as personal records of clients or risks of theft of laptops or back-ups. Encrypting these files "at rest" helps to protect them where physical security measures are failing.

Encryption is also used to protect data in transit, for example, data which is transferred through networks (Internet, e-commerce), mobile phones, wireless microphones (wireless),

Bluetooth devices and ATMs. In recent years there have been numerous reports of intercepted data in transit. Encrypting data before send them helps to secure traffic, because it is difficult to ensure physical security to all networks.

A *cryptographic algorithm*, or *cipher*, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a *key*—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

Cryptography can be divided into two major classes according to the period when they were discovered: classical cryptography and modern cryptography.

Before computers, cryptography consisted of character-based algorithms and we are talking about classical cryptography. Different cryptographic algorithms either substituted characters for one another or transposed characters with one another. The better algorithms did both, many times each. So, we have two methods: substitution and transposition.

A **substitution cipher** is one in which each character in the plaintext is substituted for another character in the ciphertext. The receiver inverts the substitution on the ciphertext to recover the plaintext.

In a **transposition cipher** the plaintext remains the same, but the order of characters is shuffled around.

Things are more complex these days, but the philosophy remains the same. The primary change is that algorithms work on bits instead of characters. This is actually just a change in the alphabet size: from 26 elements to two elements, „0” and „1”; but most good cryptographic algorithms still combine elements of substitution and transposition.

Classification in modern cryptography can be made depending on the type of encryption key: Symmetric or Private-Key Systems and Asymmetric or Public-Key Systems.

II. SYMMETRIC-KEY SYSTEM

II.1. General principles

Symmetric key algorithms means that a single key used for encryption and also for decryption is distributed to all members who participate in the communication, so all parties use a copy of this key. A very important aspect in using private-key is that if we chose a large-sized key is very difficult to break the cipher.

Symmetric key cryptography can also be called *secret key cryptography* and *private key cryptography.* Figure 1 illustrates the symmetric key encryption and decryption processes.[1]

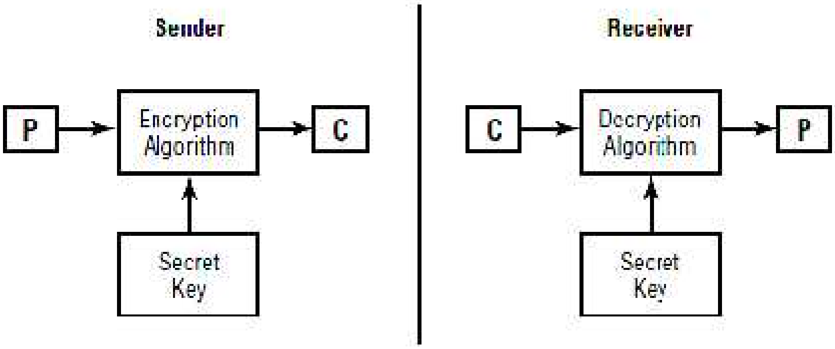


Figure 1 – Illustrating the symmetric key encryption and decryption processes

II.2. Advantages and disadvantages of using secret key encryption

Advantages of secret-key cryptography

- Symmetric-key ciphers can be designed to have high rates of data throughput. Some hardware implementations achieve encrypt rates of hundreds of megabytes per second, while software implementations may attain throughput rates in the megabytes per second range;
- Keys for symmetric-key ciphers are relatively short;
- Symmetric-key ciphers can be employed as primitives to construct various cryptographic mechanisms including pseudorandom number generators, hash functions, and computationally efficient digital signature schemes;
- Symmetric-key ciphers can be composed to produce stronger ciphers;
- The major strength of symmetric key cryptography is the great speed at which it can operate. Symmetric keying is very fast, often 1,000 to 10,000 times faster than asymmetric. By nature of the mathematics involved, symmetric key cryptography also naturally lends itself to hardware implementations, creating the opportunity for even higher-speed operations.

Disadvantages of secret-key cryptography

- Key distribution is a major problem. Parties must have a secure method of exchanging the secret key before establishing communications with the symmetric key protocol. If a secure electronic channel is not available, an offline key distribution method must often be used;

[1] James Michael Stewart, Ed Tittel, Mike Chapel – *Certified Information Systems Security Professional,* Publisher Wiley Publishing, Inc., page 353

- Symmetric key cryptography does not implement nonrepudiation. Because any communicating party can encrypt and decrypt messages with the shared secret key, there is no way to tell where a given message originated;
- The algorithm is not scalable. It is extremely difficult for large groups to communicate using symmetric key cryptography. Secure private communication between individuals in the group could be achieved only if each possible combination of users shared a private key;
- Keys must be regenerated often. Each time a participant leaves the group, all keys that involved that participant must be discarded;

III. ASYMMETRIC-KEY SYSTEM

III.1. General principles

Public key algorithms, provide a solution to the weaknesses of symmetric key encryption. In these systems, each user has two keys: a public key, which is shared with all users, and a private key, which is kept secret and known only to the user. The public key is used to encrypt the message and only the secret key can decrypt it. Figure 2 shows the algorithm used to encrypt and decrypt messages in a public key cryptosystem.[2]

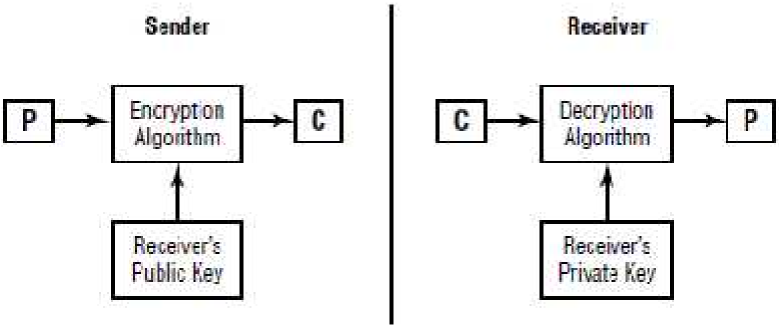


Figure 2 – Illustrating the asymmetric key encryption and decryption processes

To be better understood, we take the example of an encrypted message exchange between two people. The first person creates the message and then encrypts it using second person's public key. The only possible way to decrypt this cipher-text is to use second person's private key, and the only user with access to that key is this person. The first person can't even decrypt the message herself after she encrypts it . If the second person wants to send a reply, she simply encrypts the message using first person's public key, and then the first person reads the message by decrypting it with her private key.

[2] James Michael Stewart, Ed Tittel, Mike Chapel – *Certified Information Systems Security Professional,* Publisher Wiley Publishing, Inc., page 354

Asymmetric key algorithms also provide support for digital signature technology. Basically, if the second person wants to assure other users that a message with his name on it was actually sent by her, she first creates a message digest by using a hashing algorithm (you'll find more on hashing algorithms in chapter 5), after that she encrypts that digest using her private key. Any user who wants to verify the signature simply decrypts the message digest using public key of that person and then verifies that the decrypted message digest is accurate.

III.2. Advantages and disadvantages of using public key encryption

Advantages of public-key cryptography

- Only the private key must be kept secret (authenticity of public keys must, however, be guaranteed);
- Users can be removed far more easily from asymmetric systems. Asymmetric algorithms provide a key revocation mechanism that allows a key to be canceled, effectively removing a user from the system;
- Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable periods of time, e.g., many sessions (even several years);
- Asymmetric key encryption can provide integrity, authentication, and nonrepudiation. If a user does not share their private key with other individuals, a message signed by that user can be shown to be accurate and from a specific source and cannot be later repudiated;
- No preexisting communication link needs to exist. Two individuals can begin communicating securely from the moment they start communicating. Asymmetric cryptography does not require a preexisting relationship to provide a secure mechanism for data exchange;
- In a large network, the number of keys necessary may be considerably smaller than in the symmetric-key scenario;
- Key distribution is a simple process. Users who want to participate in the system simply make their public key available to anyone with whom they want to communicate. There is no method by which the private key can be derived from the public key;
- The addition of new users requires the generation of only one public-private key pair. This same key pair is used to communicate with all users of the asymmetric cryptosystem. This makes the algorithm extremely scalable.

Disadvantages of public-key cryptography

- The major weakness of public key cryptography is its slow speed of operation. For this reason, many applications that require the secure transmission of large amounts of data use public key cryptography to establish a connection and then exchange a symmetric secret key. The remainder of the session then uses symmetric cryptography;

- Key sizes are typically much larger than those required for symmetric-key encryption, and the size of public-key signatures is larger than that of tags providing data origin authentication from symmetric-key techniques;
- No public-key scheme has been proven to be secure.

IV. KEY MANAGEMENT

Key management is the set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties.[3]

Key management encompasses techniques and procedures supporting:

1. initialization of system users within a domain;
2. generation, distribution, and installation of keying material;
3. controlling the use of keying material;
4. update, revocation, and destruction of keying material;
5. storage, backup/recovery, and archival of keying material.

We should give a great importance in chosing an encryption key and the length of that key should balances our security requirements with performance considerations. Also, it is very important that the key to be truly random. Any patterns within the key increase the likelihood that an attacker will be able to break your encryption and degrade the security of your cryptosystem.

When using public key encryption,we must keep our secret key secret! We must not, under any circumstances, allow anyone else to gain access to your private key, because, allowing someone access even once permanently compromises all communications that take place (past, present, or future) using that key and allows the third party to successfully impersonate you.

We should not use a key for a very long time. Many organizations have mandatory key rotation requirements to protect against undetected key compromise. If you don’t have a formal policy that you must follow, select an appropriate interval based upon the frequency with which you use your key. A major advantage in changing encryption key is that there is less damage if the key is exposed. Also, an attacker has less ciphertext available that was generated under on key, which can make cryptographic attacks much more difficult

Backing up our key will help us if you lose the file containing your secret key because of data corruption, disaster, or other circumstances. You can do this by creating your own backup or

[3] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone – *Handook of Applied Cryptography*, pag. 560

using a key escrow service that maintains the backup for you. In either case, ensure that the backup is handled in a secure manner.

Keys are basically really big numbers. Key size is measured in bits; the number representing a 2048-bit key is huge. In public-key cryptography, the bigger the key, the more secure the cipher text. However, public key size and conventional cryptography's secret key size are totally unrelated. A conventional 80-bit key has the equivalent strength of a 1024- bit public key.

A conventional 128-bit key is equivalent to a 3000-bit public key. Again, the bigger the key, the more secure, but the algorithms used for each type of cryptography are very different. While the public and private keys are mathematically related, it's very difficult to derive the private key given only the public key; however, deriving the private key is always possible given enough time and computing power. This makes it very important to pick keys of the right size; large enough to be secure, but small enough to be applied fairly quickly.

One of the major problems underlying symmetric encryption algorithms is the secure distribution of the secret keys required to operate the algorithms. We can use an offline distribution or using Public Key Encryption. The first method is the simplest because involves the physical exchange of key material. One party provides the other party with a sheet of paper or piece of storage media containing the secret key. In many hardware encryption devices, this key material comes in the form of an electronic device that resembles an actual key that is inserted into the encryption device.

Many people use public key encryption to set up an initial communications link. Once the link is successfully established and the parties are satisfied as to each other's identity, they exchange a secret key over the secure public key link. They then switch communications from the public key algorithm to the secret key algorithm and enjoy the increased processing speed. In general, secret key encryption is 1,000 times faster than public key encryption.

V. HASH FUNCTIONS

Cryptographic hash functions play a fundamental role in modern cryptography. Using hash we can easily asure integrity of our encrypted messages. A hash function takes a message of variable-length as input, even thousands or millions of bits—and produces an output referred to as a *hashcode*, *hash-result*, *hash-value*, or simply *hash.* More precisely, a hash function h maps bitstrings of arbitrary finite length to strings of fixed length, say n bits. In this way we are asured that, if the information is changed in any way—even by just one bit—an entirely different output value is produced. The basic idea of cryptographic hash functions is that a hash-value serves as a compact representative image (sometimes called an *imprint*, *digital fingerprint*, or *message digest*) of an input string, and can be used as if it were uniquely identifiable with that string. The hash value corresponding to a particular message x is computed at time T_1. The integrity of this hash-value (but not the message itself) is protected in some manner. At a subsequent time T_2, the following test is carried out to determine whether the message has been altered, i.e., whether a message x' is the same as the original message. The hash-value of x' is computed and compared to the protected hash-value; if they are equal, one accepts that the inputs are also equal, and thus that the message has not been altered.

Hash functions are used for data integrity in conjunction with digital signature schemes, where for several reasons a message is typically hashed first, and then the hash- alue, as a representative of the message, is signed in place of the original message.

A distinct class of hash functions, called message authentication codes (MACs), allows message authentication by symmetric techniques. MAC algorithms take two distinct inputs, a message and a secret key, and produce a fixed-size of *n*-bits output, which in practice it is imposible to produce the same output without knowledge of the key. MACs can be used to provide data integrity and symmetric data origin authentication, as well as identification in
symmetric-key schemes.

A hash function classification can be made depending on the input data for its application, and may be split into two classes: *unkeyed hash functions*, whose specification dictates a single input parameter (a message); and *keyed hash functions*, whose specification dictates two distinct inputs, a message and a secret key.[4]

Speaking about classification, a more goal-oriented one of hash functions (beyond *keyed* vs. *unkeyed*) is necessary, based on further properties they provide and reflecting requirements of specific applications. Of the numerous categories in such a *functional classification*, two types of hash functions are considered in detail in this chapter:

1. *modification detection codes* (MDCs)

Also known as *manipulation detection codes*, and less commonly as *message integrity codes* (MICs), the purpose of an MDC is (informally) to provide a representative image or *hash* of a message. MDCs are a subclass of *unkeyed* hash functions, and themselves may be further classified; the specific classes of MDCs are:

(i) *one-way hash functions* (OWHFs): for these, finding an input which hashes to a pre-specified hash-value is difficult;

(ii) *collision resistant hash functions* (CRHFs): for these, finding any two inputs having the same hash-value is difficult.

2. *message authentication codes* (MACs)

[4] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone – *Handook of Applied Cryptography*, pag. 340

The purpose of a MAC is (informally) to facilitate, without the use of any additional mechanisms, assurances regarding both the source of a message and its integrity . MACs have two functionally distinct parameters, a message input and a secret key; they are a subclass of *keyed* hash functions.

It is generally assumed that the algorithmic specification of a hash function is public knowledge. Thus in the case of MDCs, given a message as input, anyone may compute the hash-result; and in the case of MACs, given a message as input, anyone with knowledge of the key may compute the hash-result.

Hash Function has some properties, which are listed below, and to understand better what do those mean we will use for inputs x , x' and for outputs y, y'.

1. *preimage resistance* - for essentially all pre-specified outputs, it is computationally infeasible to find any input which hashes to that output, i.e., to find any preimage x' such that h(x') = y when given any y for which a corresponding input is not known;
2. *2nd-preimage resistance* - it is computationally infeasible to find any second input which has the same output as any specified input, i.e., given x, to find a 2nd-preimage $x' \neq x$ such that h(x) = h(x');
3. *collision resistance* - it is computationally infeasible to find any two distinct inputs x, x' which hash to the same output, i.e., such that h(x) = h(x').

Objectives of adversaries vs. MDCs

The objective of an adversary who wishes to "attack" an MDC is as follows:

- to attack a OWHF: given a hash-value y, find a preimage x such that y = h(x); or given one such pair (x, h(x)), find a second preimage x' such that h(x') = h(x);
- to attack a CRHF: find any two inputs x, x', such that h(x') = h(x).

Objectives of adversaries vs. MACs

The corresponding objective of an adversary for a MAC algorithm is as follows:

- to attack a MAC: without prior knowledge of a key k, compute a new text-MAC pair

(x, $h_k(x)$) for some text x'= x_i, given one or more pairs (x_i, $h_k(x_i)$).

Computation-resistance here should hold whether the texts xi for which matching MACs are available are given to the adversary, or may be freely chosen by the adversary. Similar to the situation for signature schemes, the following attack scenarios thus exist for MACs, for adversaries with increasing advantages:

1. *known-text attack*. One or more text-MAC pairs (x_i, $h_k(x_i)$) are available.
2. *chosen-text attack*. One or more text-MAC pairs (x_i, $h_k(x_i)$) are available for x_i chosen by the adversary.

3. *adaptive chosen-text attack*. The xi may be chosen by the adversary as above, now allowing successive choices to be based on the results of prior queries.

As a certificational checkpoint,MACs should withstand adaptive chosen-text attack regardless of whether such an attack may actually be mounted in a particular environment. Some practical applications may limit the number of interactions allowed over a fixed period of time, or may be designed so as to compute MACs only for inputs created within the application itself; others may allow access to an unlimited number of text-MAC pairs, or allow MAC verification of an unlimited number of messages and accept any with a correct MAC for further processing.

Types of forgery (selective, existential)

When MAC forgery is possible (implying the MAC algorithm has been technically defeated), the severity of the practical consequences may differ depending on the degree of control an adversary has over the value x for which a MAC may be forged. This degree is differentiated by the following classification of forgeries:

1. *selective forgery* – attacks whereby an adversary is able to produce a new text-MAC pair for a text of his choice (or perhaps partially under his control). Note that here the selected value is the text for which a MAC is forged, whereas in a chosen-text attack the chosen value is the text of a text-MAC pair used for analytical purposes (e.g., to forge a MAC on a distinct text);
2. *existential forgery* – attacks whereby an adversary is able to produce a new text-MAC pair, but with no control over the value of that text.

Key recovery of the MAC key itself is the most damaging attack, and trivially allows selective forgery. MAC forgery allows an adversary to have a forged text accepted as authentic. The consequences may be severe even in the existential case. A classic example is the replacement of a monetary amount known to be small by a number randomly distributed
between 0 and $2^{32} - 1$. For this reason, messages whose integrity or authenticity is to be verified are often constrained to have pre-determined structure or a high degree of verifiable redundancy, in an attempt to preclude meaningful attacks.

Analogously to MACs, attacks on MDC schemes (primarily 2nd-preimage and collision attacks) may be classified as selective or existential. If the message can be partially controlled, then the attack may be classified as partially selective .

VI. DIGITAL SIGNATURE

VI.1. General principles

Digital signatures enable the recipient of information to verify the authenticity of the information's origin, and also verify that the information is intact. Thus, public key digital signatures provide *authentication* and data *integrity*. A digital signature also provides *non-repudiation*, which means that it prevents the sender from claiming that he or she did not actually send the information. These features are every bit as fundamental to cryptography as privacy, if not more.

A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior to a handwritten signature in that it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as to the identity of the signer.[5]

Some people tend to use signatures more than they use encryption. For example, you may not care if anyone knows that you just deposited $1000 in your account, but you do want to be darn sure it was the bank teller you were dealing with.

VI.2. Signing documents with Symmetric Cryptosystems and an Arbitrator

Let's take three persons: Alice , Bob and Jack. Alice wants to sign a digital message and send it to Bob. With the help of Jack and a symmetric cryptosystem, she can. Jack is a powerful, trusted arbitrator. He can communicate with both Alice and Bob (and everyone else who may want to sign a digital document). He shares a secret key, K_A, with Alice, and a different secret key, K_B, with Bob. These keys have been established long before the protocol begins and can be reused multiple times for multiple signings.

(1) Alice encrypts her message to Bob with K_A and sends it to Jack.

(2) Jack decrypts the message with K_A.

(3) Jack takes the decrypted message and a statement that he has received this message from Alice, and encrypts the whole bundle with K_B.

(4) Jack sends the encrypted bundle to Bob.

(5) Bob decrypts the bundle with K_B. He can now read both the message and Jack's certification that Alice sent it.

Jack knows that the message is from Alice because only he and she share their secret key and only Alice could encrypt a message using it. This is a good way of proving authentication and data integrity, because:

[5] Network Associates, Inc. and its Affiliated Companies – *An introduction to Cryptography*, page 18

(1) This signature is authentic. Jack is a trusted arbitrator and he knows that the message came from Alice. Jack's certification serves as proof to Bob.

(2) This signature is unforgeable. Only Alice (and Jack, but everyone trusts him) knows K_A, so only Alice could have sent Jack a message encrypted with K_A. If someone tried to impersonate Alice, Jack would have immediately realized this in step (2) and would not certify its authenticity.

(3) This signature is not reusable. If Bob tried to take Jack's certification and attach it to another message, an arbitrator (it could be Jack or it could be a completely different arbitrator with access to the same information) would ask Bob to produce both the message and Alice's encrypted message. The arbitrator would then encrypt the message with K_A and see that it did not match the encrypted message that Bob gave him. Bob, of course, could not

produce an encrypted message that matches because he does not know K_A.

(4) The signed document is unalterable. Were Bob to try to alter the document after receipt, Jack could prove that he tried to cheat in exactly the same manner just described.

(5) The signature cannot be repudiated. Even if Alice later claims that she never sent the message, Jack's certification says otherwise.

If Bob wants to show Carmen a document signed by Alice, he can't reveal his secret key to her. He has to go through Jack again:

(1) Bob takes the message and Trent's statement that the message came from Alice, encrypts them with K_B, and sends them back to Jack.

(2) Jack decrypts the bundle with K_B.

(3) Jack checks his database and confirms that the original message came from Alice.

(4) Jack re-encrypts the bundle with the secret key he shares with Carmen, K_C, and sends it to her.

(5) Carmen decrypts the bundle with K_C. She can now read both the message and Jack's certification that Alice sent it.

These protocols work, but they're time-consuming for Jack. He must spend his days decrypting and encrypting messages, acting as the intermediary between every pair of people who want to send signed documents to one another. He must keep a database of messages (although this can be avoided by sending the recipient a copy of the sender's encrypted message).

Harder still is creating and maintaining someone like Jack, someone that everyone on the network trusts. Trent has to be infallible; if he makes even one mistake in a million signatures, no one is going to trust him. Trent has to be completely secure. If his database of secret keys ever got out or if someone managed to modify his programming, everyone's signatures would be completely useless.

VI.3. Signing documents with Public-Key Cryptography

There are public-key algorithms that can be used for digital signatures. In some algorithms either the public key or the private key can be used for encryption. Encrypt a document using your private key, and you have a secure digital signature. In other cases, there is a separate algorithm for digital signatures that cannot be used for encryption.

The basic protocol is simple:

(1) Alice encrypts the document with her private key, thereby signing the document;

(2) Alice sends the signed document to Bob;

(3) Bob decrypts the document with Alice's public key, thereby verifying the signature.

This protocol is far better than the previous one. Jack is not needed to either sign or verify signatures, because if Bob cannot perform step (3), then he knows the signature is not valid.

This protocol also satisfies the following characteristics:

(1) The signature is authentic; when Bob verifies the message with Alice's public key, he knows that she signed it;

(2) The signature is unforgeable; only Alice knows her private key;

(3) The signature is not reusable; the signature is a function of the document and cannot be transferred to any other document;

(4) The signed document is unalterable; if there is any alteration to the document, the signature can no longer be verified with Alice's public key.

(5) The signature cannot be repudiated. Bob doesn't need Alice's help to verify her signature.

VI.4. Signing documents with Public-Key Cryptography and One-Way Hash Functions

In practical implementations, public-key algorithms are often too inefficient to sign long documents. To save time, digital signature protocols are often implemented with one-way hash functions. Instead of signing a document, Alice signs the hash of the document. In this protocol, both the one-way hash function and the digital signature algorithm are agreed upon beforehand.

(1) Alice produces a one-way hash of a document;

(2) Alice encrypts the hash with her private key, thereby signing the document;

(3) Alice sends the document and the signed hash to Bob;

(4) Bob produces a one-way hash of the document that Alice sent. He then, using the digital signature algorithm, decrypts the signed hash with Alice's public key. If the signed hash matches the hash he generated, the signature is valid.

Speed increases drastically and, since the chances of two different documents having the same *n*-bit hash are only one in 2^n, anyone can safely equate a signature of the hash with a signature of the document. If a non-one-way hash function were used, it would be an easy matter to create multiple documents that hashed to the same value, so that anyone signing a particular document would be cheated into signing a multitude of documents.[6]

This protocol has other benefits. First, the signature can be kept separate from the document. Second, the recipient's storage requirements for the document and signature are much smaller. An archival system can use this type of protocol to verify the existence of documents without storing their contents. The central database could just store the hashes of files. It doesn't have to see the files at all; users submit their hashes to the database, and the database timestamps the submissions and stores them. If there is any disagreement in the future about who created a document and when, the database could resolve it by finding the hash in its files.

CONCLUSIONS

Assuring data security is not an easy job and implies not choosing only a suitable algorithm and the perfect key length but also other method to meet the four fundamental goals: confidentiality, integrity, authentication, and nonrepudiation.

It is always the responsibility of the sender to ensure that proper mechanisms are in place to ensure that the security and privacy of a message or transmission are maintained.

When you work in data security, it's important that you comply with several best practice requirements to maintain the security of your communications. First, choose your encryption system wisely. Choose an encryption system with an algorithm in the public domain that has been thoroughly vetted by industry experts. Be wary and don't be satisfied only in using encryption method for your data privacy but also use over methods of cryptography.

To summarize everything I said before you have to account for these:

- If you need confidentiality when sending an email message or only protect the data from your computer, then encrypt the message/data;
- If your message must maintain integrity, then you must hash the message;
- If your message needs authentication and integrity, then you should digitally sign the message;

[6] Bruce Scheiner – *Applied cryptography, second edition,* Publisher John Wiley & Sons, Inc., 1996, page 68

- If your message requires confidentiality, integrity, authentication, and nonrepudiation, then you should encrypt and digitally sign the message.

REFERENCES

1. James Michael Stewart, Ed Tittel, Mike Chapel – *Certified Information Systems Security Professional,* Publisher Wiley Publishing, Inc., 2008;
2. Bruce Scheiner – *Applied cryptography, second edition,* Publisher John Wiley & Sons, Inc., 1996;
3. Network Associates, Inc. and its Affiliated Companies – *An introduction to Cryptography;*
4. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone – *Handook of Applied Cryptography,* 1996;
5. Christof Paar, Jan Pelzl – *Understanding Cryptography*, Publisher Springer, 2010;
6. Oded Goldreich – *Foundations of Cryptography II Basic Applications*, Publisher Cambridge University Press, 2009;
7. http://www.di-mgt.com.au/cryptokeys.html, 10.06.2011.

INFORMATION ASSURANCE - INTELLIGENCE - INFORMATION SUPERIORITY RELATIONSHIP

LTC Ioan-Mihai ILIEŞ

INTRODUCTION

In this paper we aimed at achieving short of a general theoretical framework concerning the relationship between information & information assurance - intelligence - information superiority, which contribute to enhancing knowledge about the preparation and execution of operations in multinational environment. For this, following the ideas outlined during the postgraduate Information Security Management Course within the Department of Regional Resource Management Studies in National Defense University "Carol I" and scientific advisor recommended bibliography study, we have made a plan to address this paper in three chapters. All the information contained in this course final paper are unclassified or public.

In chapter 1, we have analyzed the terms "security of information", "information security (INFOSEC)" and "information assurance" through the NATO Security Directive, the practice gained in this regard by the U.S. Army, by the National Army as well as some international players, non-military personnel, concerned in the area of information security, in order to make a comparison in this respect. In Chapter 2 we presented some considerations on the role of intelligence within NATO and principles with emphasis the data – information -intelligence relationship within NATO, the role of NATO intelligence cycle, the presentation of combat intelligence functions within NATO and the U.S. Army, and how information security affects the military intelligence cycle. In Chapter 3 we emphasized the need for information security during the information operations conducted by the Alliance, with an accent on explaining the relationship between information security, intelligence cycle in NATO operations, the role of information security to achieve and maintain information superiority in NATO and presentation of lessons learned for commanding, staff and information officers on security of information generated by the intelligence structures in Iraqi theater of operations.

We expressed agreement or disagreement on some issues mentioned in the doctrines, manuals, courses, studies or in the papers of the author and where I found it necessary and useful we have exposed their own opinions.

The use of specific military art and science terminology, with emphasis on terminology of information & information security, intelligence and information superiority, in the present study appear sometimes different names for the same concepts. This is due to various bibliographic sources, the accuracy of the approach of our ideas imposing unchanged authors quotes for these sources. Of course, we must take into account the fact that the evolution of these terms has been continued until the emergence of the Romanian Army Doctrine for Information in 2005 and it takes place today too. Therefore, we mention that in this paper, the terms information and intelligence are not synonymous. Moreover, consider that they should analyze through the data - information - (products) intelligence - relevant information - execution information relationship, which we have detailed it in this paper. It is natural to face a military theory of strong dynamics in the context of powerful transformations that the Romanian Army suffers from the perspective that we are members of NATO, but to clarify some basic concepts requires an urgent necessity.

Another important aspect that we wish to express on this course final paper is that for a better understanding of specific concepts in paragraphs dealing with operating systems / functions of fighting in general and operating system / fighting function in particular, we made a comparison between the provisions of, NATO and the U.S. and Romanian battle manuals, detailing the issues we thought were most important in the annexes to this paper. However, it is necessary an indication of a general nature: not all the provisions of NATO and American manuals can be applied also in the Romanian military doctrines (for different reasons from the mentality, to the level of technical training and equipment to fight).

Addressing the final paper issues according to information - information security - intelligence and analyzing the NATO, U.S. and national doctrines, we can say that there is not essentially differentiates between us and our allies. But on the practical approach to these doctrines, some allies (e.g. Americans, British and German) are much better organized, the deepening problems of each type of work being done in other military doctrines, indicated when necessary. For these reasons, when I studied the doctrines of NATO and U.S. intelligence we had a clear impression, without repetitions, additions or changes about the operational language I have learned and analyzed in depth the specific problems of each military activity studying the specific field manuals, when necessary . Another aspect to note is that a problem is treated in a manual the same like in other manuals, without extra changes or additions.In the end the introduction, we consider that the SOP - Standing Operating Procedure drawn up by military intelligence structure (especially the chapter on information / intelligence), except that clearly sets out the steps to be followed in planning the operation for the information / intelligence personnel Staff, is at present, a solution adopted by the commander of necessity. Commander finds himself in an uncomfortable position to make a summary of the provisions of intelligence treated differently in some manuals to optimize military decision making process so that, finally, to achieve the desire proposed end-state: inclusion in the higher echelon commander's intention and executing the mission received from him.

Thus, we try to present in this paper as our own understanding, elements, phenomena and processes in accordance with information security - information superiority relationship, for a better knowledge of the NATO operations mechanism.

1. SECURITY OF INFORMATION, INFORMATION SECURITY AND INFORMATION ASSURANCE IN A MULTINATIONAL ENVIRONMENT

In the beginning, we believe it useful to mention that security of information, information security and information assurance are not identical. To highlight the basic idea of this work must be noted from the outset that there are two types of approach to information security. According to NATO doctrine, the U.S. ground forces and national, we analyze terms "security of information", "information security" and “information assurance”. In other words, in chapter 1, we have analyzed the terms "security of information", "information security (INFOSEC)” and “information assurance” through the NATO Security Directive, the practice gained in this regard by the U.S. Army, by the National Army as well as some international players, non-military personnel, concerned in the area of information security, in order to make a comparison in this respect.

1.1. Security of information, information security and information assurance within NATO security directives

For explaining the meanings of the terms of interest in this chapter, we will use the original Security directive within NATO CM(2002)49[7].

Information = knowledge that can be communicated in any form.

Information assurance[8] (IA) = measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Security of information[9] = the application of general security measures and procedures to prevent detect and recover from the loss or compromise of information. Classified information

[7] Security within the North Atlantic Treaty Organization, C-M(2002)49 dated 17 June 2002, http://www.statewatch.org/news/2006/sep/nato-sec-classifications.pdf .

[8] CNSS Instruction No. 4009, 26 April 2010, National Information Assurance (IA) Glossary, p.35, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf .

[9] Corrigendum to C-M(2002)49 Security within the North Atlantic Treaty Organization, C-M (2002)49 dated 17 June 2002dated, Amendment 7, p. 5, http://www.nbu.cz/_downloads/pravni-predpisy---nato/container-nodeid-751/c-m200249-cor3-nu-pd-security-within-the-north-atlantic-.pdf, .

shall be protected throughout its life cycle to a level commensurate with its level of classification. It shall be managed to ensure that it is appropriately classified, is clearly identified as classified and remains classified only as long as this is necessary.

Information security (INFOSEC) = the application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves.

Notes:

1. INFOSEC measures include those of computer, transmission, emission and cryptography security.
2. Such measures also include detection, documentation and countering of threats to information and to the systems.

Information system (IS)[10] = the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Information superiority[11] = that degree of dominance in the information domain which permits the conduct of operations without effective opposition.

Information warfare (IW)[12] = **i**nformation operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Classified information = any information (namely, knowledge that can be communicated in any form) or material determined to require protection against unauthorized disclosure and which has been SO designated by a security classification.

Material = documents and also any item of machinery or equipment or weapons either manufactured or in the process of manufacture.

Document = any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions by an means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media, and removable computer storage media.

[10] Department of Defense Dictionary of Military and Associated Terms, 2001, amended through 2003, p.255.

[11] Ibidem.

[12] Ibidem.

Confidentiality = the property that information is not made available or disclosed to unauthorized individuals or entities.

Availability = the property of information and material being accessible and usable upon demand by an authorized individual or entity.

Integrity = the property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorized manner.

In other words, information assurance „is in charge" with entire information flow within an specific in information system, while security of information ensures protective measures of all types of information in generally, providing „CIA" for all – source - information (in this case, „CIA" means **C**onfidentiality, **I**ntegrity and **A**vailability).

Security classifications it is a very important issue for protection of information. They shall be applied to information to indicate the possible damage to the security of NATO and/or its member nations if the information is subjected to unauthorized disclosure.

When classifying information, the originator shall know that damage means if the information is subjected to unauthorized disclosure, and shall indicate whether their information can be downgraded or declassified on a certain date or event.

Information security (INFOSEC) [13] is the application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems. For this reason, in order to achieve the confidentiality, integrity and availability for classified information within electronic systems, a crystal clear set of security measures (physical, personnel, security of information and INFOSEC) shall be implemented to assure a secure environment in which to operate a communication, information or other electronic system.

In the same time, security of information, INFOSEC & IA have to offer protection of information on the military structure key points. The publication of information about civilian installations (defense supplies, energy supply, etc.) of military significance in times of tension or war may assist bombing, sabotage or terrorist attack by allowing potential enemies to compile a key points list, and to identify points vulnerable to sabotage or terrorism within individual key points. Policy should be designed to hamper the compilation by potential enemies of a Key Points List, to allow the invocation of security exemptions from publication of relevant data, and to encourage awareness of the risks among installation owners and operators.

[13] Security within the North Atlantic Treaty Organization, C-M(2002)49 dated 17 June 2002, p.6, http://www.statewatch.org/news/2006/sep/nato-sec-classifications.pdf .

On the other hand, INFOSEC policy **sets out the minimum standards** for the protection of multinational environment (ME) classified information, and supporting system services and resources' in communication, information and other electronic systems storing, processing or transmitting classified information.

The "Primary Directive on INFOSEC - Security within the North Atlantic Treaty Organization, C-M(2002)49 dated 17 June 2002" is supported by directives addressing INFOSEC management (including security risk management, security approval, security-related documentation, and security review / inspection) and INFOSEC technical and implementation aspects (including computer and local area network (LAN) security, interconnection of networks security, cryptography security, transmission security, and emission security).

According to CM(2002)49, Enclosure F, the main security objectives for achieving adequate security protection of NATO classified information handled in systems and set of security measures (physical, personnel, information and INFOSEC) shall ensure the information confidentiality, integrity and availability by controlling the disclosure and access of classified information and supporting system services and resources[14];

The integrity and availability of classified information and of supporting system services and resources shall be protected by a minimum set of measures aimed at ensuring general protection against commonly problems that can affect all electronic systems. Additional measures shall be taken, where a risk assessment has established that classified information is subject to increased risks from specific threats and vulnerabilities.

In this respect, we stress the main domains for achieving and maintaining a high level for ensuring the information confidentiality, integrity and availability of information:

- **security approval** of any process for an adequate level of INFOSEC and protection of communications and information systems that convey classified information;
- **personnel security**, that ensure only authorized access to classified information in any form for individuals which are security cleared;
- **physical security**, that ensure only protected areas in which classified information is presented or handled using information technology, or where potential access to such information is possible;

[14] Supporting System Services and Resources - those services and resources required to ensure that the security objectives of the systems are achieved; to include, for example, cryptography mechanisms and equipments, COMSEC materials, directory services, and environmental facilities and controls.

- **security of computer storage media** for all classified computer storage media that shall be properly identified, stored and protected in a manner commensurate with the highest classification of the stored information;
- **accountability** that shall be a means to provide sufficient information to be able to investigate a deliberate or accidental compromise of the confidentiality of accountable information;
- **security measures** for all systems handling classified information, that shall be applied to meet the security objectives, and to protect information. The security measures shall include:
  - means to reliably identify and authenticate persons authorized access;
  - means to control disclosure and access to information based upon the need-to-know principle;
  - means to verify the integrity and origin of information;
  - means to maintain the confidentiality, integrity, availability of classified information;
  - means to control the connection of systems handling classified information;
  - determination of the confidence to be placed in the INFOSEC protection mechanisms;
  - means to assess and verify the proper functioning of the INFOSEC protection mechanisms over the life-cycle of the system;
  - means to investigate user and system activity.
- **security management** mechanisms and procedures shall be implemented to deter, prevent and detect the incidents affecting the confidentiality, integrity and availability of classified information, including the reporting of security incidents;
- **security risk management** of all systems handling classified information.
- **electromagnetic transmission** of classified information protecting transmissions from detection, interception or exploitation. When necessary, cryptography methods are required to provide protection confidentiality, integrity and availability of information;
- **emission security** shall be implemented to protect against the compromise of information classified NC and above through unintentional electromagnetic emissions. The measures shall be commensurate with the risk of exploitation and the sensitivity of the information that these individuals receive appropriate security education and training.

According to AC/35-D/2002, a NATO directive in support of Enclosure E of CM(2002)49, INFOSEC[15] means:

- identification and authentication/access control - only authorized users, who have been uniquely and reliably identified and authenticated, shall have access to relevant classified information, whether this is national, other organization, NATO or CJTF;
- accounting/audit - authorized users shall be individually **accountable** for their access (read, write, modify and delete) and actions (transmit/receive) with regard to classified information within the CJTF. Measures will be implemented by the CJTF security authorities (as specified in the OPORD) to detect and prevent users or bodies (inside or outside the CJTF) from breaching or attempting to breach the security environment;
- confidentiality - measures shall be taken to prevent the interception or redirection of data communications that carry classified information within the CJTF;
- integrity - the integrity of all classified information stored, processed or transmitted within the CJTF shall be maintained;
- availability - classified information within the CJTF shall be available to authorized users when required.

Another kind of approach for a clearly understanding of security of information and for achieving a very good level for security of classified information, a clear access authorization must be established. The security official will inform personnel of their level of access to classified material and whether they are authorized to access classified information. Additionally, security structure should maintain a list indicating the levels of access for each assigned individual who is authorized access to NATO information and verify NATO access authorizations for all personnel**. *In our opinion, as with classified information, access is not based on duty position, rank, or level of clearance. Access is based on need-to-know, the proper level of clearance, and an access briefing for a specific level and type of classified information.***

Other way for security of information, information security & information assurance analysis is provided to us by the NATO Programme for Security through Science. In 2004, the NATO

[15] AC/35-D/2002-REV2, Appendix 6, Annex 1, p. 1-52, http://www.nbf.hu/anyagok/jogszabaly/AC_35-D_2002-REV2.pdf

[15] The NATO Programme for Security through Science, Information and Communications Security: Information and Communications Security Supporting cooperation on information systems and communications networks, p.1, http://www.nato.int/science/publication/pdf/ics_en.pdf

Science Programme[16] was redirected to promote security-related science and technology, thereby better reflecting the changed environment in which NATO now finds itself. The new NATO Programme for Security through Science contributes to security, stability and solidarity among nations. The Programme offers support for collaboration on research areas of defense against terrorism or countering other threats to security. Grant NATO invites applications for unclassified activities on topics related to the following specific areas:

- encouraging security awareness: the objective is to raise security awareness by organizing *security workshops*, by *stimulating risk assessment* and *managing risks* and by assisting Partner countries in the development of *policies and standards* in this area;
- infrastructure security and reliability: the objective is the development of *security tools* and *network services*, in order to guarantee the security and reliability of the various elements of an infrastructure.
- information security: this area relates to the security of information systems and involves *back up, physical protection, disaster contingency planning*, *identification* and *authorization issues, protection of the data* and the *privacy aspects* of its use;
- cyber crime and terrorism: this ranges from the *illegal* use of a system (including "hacking"), to *fraud* and *peculation* and to the involvement of Information and Communications Technology (ICT) systems in *terrorist acts*, both to commit and prevent them. Setting up a Computer Emergency Response Team (CERT) infrastructure to monitor and recover from attacks on a system is also considered.

1.2. Information security & information assurance within the information operations

Next, we analyze the NATO Final Report[17] from 2001 about Strategic and Organisational Implications for Euro-Atlantic Security of Information Operations. We consider that this is a cue aspect for a very clear understanding of security of information - information security (INFOSEC) - information assurance - intelligence - information superiority relationship.

[16] The NATO Programme for Security through Science, Information and Communications Security: Information and Communications Security Supporting cooperation on information systems and communications networks, p.1, http://www.nato.int/science/publication/pdf/ics_en.pdf

[17] NATO Individual Fellowship 1999/2001 Final Report Strategic and Organisational Implications for Euro-Atlantic Security of Information Operations Dr Andrew Rathmell RAND Europe (www.randeurope.org) & Information Assurance Advisory Council (www.iaac.org.uk) http://www.nato.int/acad/fellow/99-01/rathmell.pdf .

In the abstract of rhis report, is underlined that the development of Information Operations and, more particularly, Computer Network Operations (CNO), has been paralleled by calls to control both the military and the criminal/terrorist use of these capabilities. However, an unresolved dilemma faced by the leading powers; whether to exploit their CNO advantage for strategic purposes or to protect the global information environment on which depend. In resolving this dilemma, Western strategists need to take into account two important new features of the security environment - interdependency and the role of the private sector.

The above mentioned report is concerned with the prospects for the emergence of an international regime for control of Computer Network Operations (CNO). CNO are a subset of a broader set of malicious computer-mediated activities.

According to draft British military doctrine[18], CNO comprises: Computer Network Exploitation (CNE), namely: “the ability to gain access to information hosted on information systems and the ability to make use of the system itself;” Computer Network Attack (CNA), namely: the “use of novel approaches to enter computer networks and attack the data, the processes or the hardware;” and Computer Network Defence (CND), which is “protection against the enemy’s CNA and CNE and incorporates hardware and software approaches alongside people based approaches.”[1] In turn, CNO are one element of Information Operations (IO).

The report states that the precision of the military definition is not yet matched by internationally agreed definitions in the civil and criminal domains. The EU is now moving towards the concept of “cyber-abuse” as an global term to include activities ranging from privacy violations to attacks on computer systems[19]. The Council of Europe’s Cybercrime Convention, with which EU approaches are likely to be harmonised, encompasses CNA under “category 1” offences, i.e. offences “against the confidentiality, integrity and availability of computer data and systems[20].” The G-8 Government-Industry Conference on High Tech Crime has however proposed that two major categories of threat be agreed upon, namely computer infrastructure attack and computer assisted threat. The former is defined as “operations to disrupt, deny, degrade, or destroy

[18] Ministry of Defence, Draft doctrine for Information Operations; Joint Doctrine Pamphlet XX-01. Joint Doctrine and Concepts Centre, Shrivenham, 1 March 2001, p. 8.

[19] http://www.jrc.deppy.it .

[20] The other categories of offences are: 2) Computer-related offences; 3) Content-related offences; 4) Offences related to infringements of copyright and related rights.

information resident in computers and computer networks, or the computers and networks themselves. Malicious acts, unauthorized access, theft of service, denial of service[21].” [4]

Other important ideea in this report argues that a more holistic understanding of the emerging global information environment is required in order to better guide Western strategic interests and policy development. The report states that Western strategic and economic interests can best be fulfilled by developing norms of military behaviour in cyberspace.

In our opinion, after the report analyze, the most important provision of this paper relates to the strategic dilemma of westwern analysts. This strategic dilemma is a very simple one: the NATO states want to exploit their CNO advantage in the military sphere but in the same time need to protect the global information environment.

In other words, led by the USA, NATO nations are strongly interested to develop doctrines and capabilities that will allow them to exploit cyberspace for military advantage. Within the broad IO range, the experts look for to integrate CNO into routine military planning. At the same time, these nations are becoming concerned at the dependency of their militaries, governments, economies and societies on the networked information. They try to mitigate the resultant risks. The desire both to exploit and to restrict CNO is a paradox that needs to be addressed before an international regime can be developed. Underlying this paradox, the report underlines two divergent approaches.

One approach defines the CNO threat as being from organised crime, electronic vandalism, corporate espionage and sub-state terrorism. The threat is defined as being to the economic prosperity and social stability of all nations plugged into the global information infrastructure. In this paradigm, all nations have an interest in working together to devise international regimes that will ensure the trustworthiness and survivability of information networks. It is a non-zero sum game. From this perspective, a range of mechanisms can be used to mitigate the risks. International organisations can promulgate infosec standards and industry can be encouraged to make its information systems more secure and dependable.

The other approach treats control of CNO as a zero sum game. The focus is on the threat from nation states; IO and CNO are perceived as tools of strategic coercion. Although it may not be realistic to control CNE as an intelligence gathering tool, CNA that do breach the confidentiality, integrity or availability of information systems could in theory be treated as weapons of war and brought within the scope of arms control or the laws of armed conflict. In this approach, existing

[21] G8 Government/Industry Conference on High-Tech Crime, Report of Workshop 3: Threat Assessment and Prevention, Tokyo, 22-24 May 2001, p. 1-2.

mechanisms and methods such as the Laws of Armed Conflict and arms control/verification regimes could be applied to this new "weapon system."

In our opinion, despite the fact that there are many concerns very clearly expressed in this report, the strategic dilemma remains valid: volition to exploit the CNO advantage is in contradiction with the protection of the global information environment. In this respect, we have to add that the report establishes the fact that this dilemma remains unresolved is evident from the variety of activities in the Western world both in the military IO sphere and in the CND sphere (both civil and military). In other words, there are tensions between the specific institutions in pursuing the military (offensive) and civil (defensive) approaches. A very important problem is that existing state-led approaches to the military dimension of CNO fail to recognise the leading role of the private sector in this domain (and the nature of the globally interdependent network environment in our contemporary humankind).

In the final of this section, we consider that is really necessary to analyze the cyberspace protection. Accordingly, we wish to bring to attention a strong and wise idea from 9/11 Commission Report: „We learned that the institutions charged with protecting our borders, civil aviation, and national security did not understand how grave this threat[22] could be, and did not adjust their policies, plans, and practices to deter or defeat it. We learned of fault lines within our government - between foreign and domestic intelligence, and between and within agencies. We learned of the pervasive problems of managing and sharing information across a large and unwieldy government that had been built in a different era to confront different dangers[23]".

The American nation was unprepared for 9/11 terrorist attack. How did this happen, and how can be avoided such tragedy again, asked itself the commission? Approximate 5 months ago in March 2001, President Bush's National Security Adviser Condoleezza Rice noted that: "it is a paradox of our times that the very technology that makes our economy so dynamic and our military forces so dominating also makes us more vulnerable." She warned "Corrupt [the information] networks, and you disrupt this nation"[24]. The European Commission warned in March 2001 that "the information infrastructure has become a critical part of the backbone of our

[22] Terrorrist attack.

[23] The 9-11 Commission Report, http://www.9-11commission.gov/report/911Report.pdf , p. xvi

[24] AP, "National Security Adviser sees cyberterrorist threat", 26 March 2001, cited in NATO Individual Fellowship 1999/2001 Final Report Strategic and Organisational Implications for Euro-Atlantic Security of Information Operations Dr Andrew Rathmell RAND Europe (www.randeurope.org) & Information Assurance Advisory Council, p. 14 (www.iaac.org.uk) http://www.nato.int/acad/fellow/99-01/rathmell.pdf .

economies. Users should be able to rely on the availability of information services and have the confidence that their communications and data are safe from unauthorised access or modification. The take up of electronic commerce and the full realisation of Information Society depend on this"[25].

Like military officers, we have to ask ourselves what the necessary lesson learned for us it is. Apparently without a clear interconnection, these two above mentioned quotes are very strong interconnected. After 9/11 events, we can discuss about other kind of war, the war against terrorism (anti-terrorist and counter-terrorist actions). The terrorist attacks are not only by bombs and arms. Within the war against terrorism, a very important confrontation is the cyber one (as we stressed before, our contemporary society is an information society based on computer networks). Cyber confrontation means cyber attack and cyber defense. In our opinion, the cyber terrorist actions are cyber attacks. In this respect, we have to ask ourselves if we and our nation are prepared in case of a terrorist attack. The terrorists have sufficient means and determination to perform a cyber attack according to their insidious intentions. Moreover, are we prepared for a cyber terrorist attack? In our opinion, this course that is almost finished helped us to answer these questions. If we managed to build clear ideas about it, we won a very important thing.

As a result of these concerns, a complex and overlapping web of national, regional & multilateral initiatives has emerged. A common theme behind these initiatives is the recognition of the inadequacy of existing state-centric policing and legislative structures to police international networks and the importance of ensuring that private networks are secured against disruption. One way of grouping these initiatives is to use the standard information security paradigm of Deterrence; Prevention; Detection; and Reaction[26].

Deterrence: multilateral initiatives to deter CNA include harmonizing cyber-crime legislation to promote tougher criminal penalties and better e-commerce legislation (Council of Europe Convention, United Nations Commission on International Trade Law - UNCITRAL).

Prevention: multilateral initiatives to prevent CNA centre on promoting the design and use of more secure information systems (e.g. research and development - R&D initiatives between the US and EU; Common Criteria) and better information security management in both public and private sectors (e.g. International Organization for Standardization - ISO and Organization for Economic Co-operation and Development - OECD standards and guidelines initiatives). Other measures include legal and technological initiatives such as the promotion of security mechanisms (e.g. electronic signature legislation in Europe).

[25] COM(2000) 890 final, Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime cited ibidem.

[26] Ibidem

Detection: multilateral initiatives to detect CNA include the creation of enhanced cooperative policing mechanisms (e.g. The Group of Eight, G-8 national points of contact for cyber-crime). Another important area is the effort to provide early warning of cyber-attack through exchanging information between the public and private sectors (e.g. US Information Sharing & Analysis Centers, Forum for Incident Response and Security Teams - FIRST, European Early Warning & Information System).

Reaction: multilateral initiatives to react to CNA include efforts to design robust and survivable information infrastructures; development of crisis management systems; and improvement in coordination of policing and criminal justice efforts.

In conclusion, these initiatives involve significant investments of time and effort from a variety of government departments in many nations, from numerous international organisations and from numerous companies, large and small. Many initiatives are pre-existing, many are being pursued in isolation. Nonetheless, there has emerged a coherent and effective set of initiatives involving states and businesses, not to mention some NGOs, that is focused upon improving the security of the emerging global information environment.

1.3. Information security from the perspective of non - military actors

According to NATO comprehensive approach, all military or non-military parts that are involved in a multinational joint operation are important and need to be addressed together. In this respect, in the final of the chapter 1 we analyze security of information -information security relationship by analysis of one non-military structure with significant interests in information security.

This one is SysAdmin, Audit, Network, Security - SANS [27]. According to SANS Information Security Resources, information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. Wikipedia says, "Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms **information security and computer security** are frequently used interchangeably.

According to SANS, these fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the

[27] SANS SysAdmin, Audit, Network, Security, p.1 http://www.sans.org/information_security.php .

methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms."[28]

On the SANS web site, we find several courses in the information security domain:

- Security 401: Sans Security Essentials;
- Security 504: Hacker Techniques, Exploits and Incident Handling;
- Forensics 408: Computer Forensic Essentials;
- Developer/Security 542: Web App Penetration Testing and Ethical Hacking;
- Legal 523: Legal Issues in Information Technology and Information Security;
- Management 512: Sans Security Leadership Essentials For Managers;
- Management 524: Security Policy & Awareness.

SANS web site invites us to visit the SANS Security Policy Template page, a consensus research project of the SANS community. The ultimate goal of the project is to offer everything we need for rapid development and implementation of information security policies. We can find a great set of resources posted here already including policy templates for twenty-four important security requirements.

As per a non-military web-site[29] information security is the process of protecting information. It protects its availability, privacy and integrity. Access to stored information on computer databases has increased greatly. More companies store business and individual information on computer than ever before. Much of the information stored is highly confidential and not for public viewing.

Many businesses are solely based on information stored in computers. Personal staff details, client lists, salaries, bank account details, marketing and sales information may all be stored on a database. Without this information, it would often be very hard for a business to operate. Information security systems need to be implemented to protect this information.

SANS approach of the effective information security systems means that they incorporate a range of policies, security products, technologies and procedures. Software applications which provide firewall information security and virus scanners are not enough on their own to protect information. A set of procedures and systems needs to be applied to effectively deter access to information.

There are people who make a living from hacking or breaking through information security systems. They use their technological skills to break into computer systems and access private

[28] http://en.wikipedia.org/wiki/Information_security .

[29] WiseGEEK, clear answers for common questions, p.1, http://www.wisegeek.com/ .

information. Firewalls, which are designed to prevent access to a computer's network, can be bypassed by a hacker with the right hardware. This could result in the loss of vital information, or a virus could be planted and erase all information. A computer hacker can gain access to a network if a firewall is shut down for only a minute.

One of the biggest potential threats to information security is the people who operate the computers. A workplace may have excellent information security systems in place, but security can be easily compromised. If a help desk worker gives out or resets passwords without verifying who the information is for, then anyone can easily gain access to the system. Computer operators should be made fully aware of the importance of security.

Simple security measures can be used by everyone to keep data secure. Changing passwords on our computers, and using combinations of letters and numbers, makes it harder for hackers to gain access. Also, we do not keep a note of our passwords where its can be easily accessed. This is the same idea as not keeping our bank card and PIN number together. We would not want anyone to have access to the information or funds in our bank account, and it is the same with our computers.

There has never been such a thing as a totally secure system. Hackers will always find more sophisticated ways to gain access. However, with technology implementing higher levels of information security, such as iris recognition systems, security systems should keep us out for a little longer.

We consider very useful for us to take in consideration the Information Security Risks on “wiseGEEK” approach. We can find out some very interesting security issues on wise GEEK web site:

- security information responsive actions can also be used to handle a **security risk**, however, as some issues can arise regardless of preparation and should be handled quickly and effectively to reduce the impact of such issues. A digital or **information security risk** can be a major concern for many companies that utilize computers for business or record keeping.
- though measures such as camera systems, guards, response teams, employee background checks, and staff training for **security** problems are important to the **risk** management of physical businesses, the world of digital commerce requires an entirely different system. In **information** technology or IT **security risk** management, analysis and response is far less concerned with physical break ins or thefts, and more worried about the use of viruses and the potential for hacking and identity theft.

In the final of this chapter, we can conclude that there is a distinct relationship between security of information, information security and information assurance. Te first term, security of information, is related to information in generally, in other words, security of all types of information (documents, materials, electronic information and so on). (INFOSEC) is encompassed in security of information term, because information handled in electronic systems. Both these terms are included in information assurance term, referring to information systems security (see figure 1).

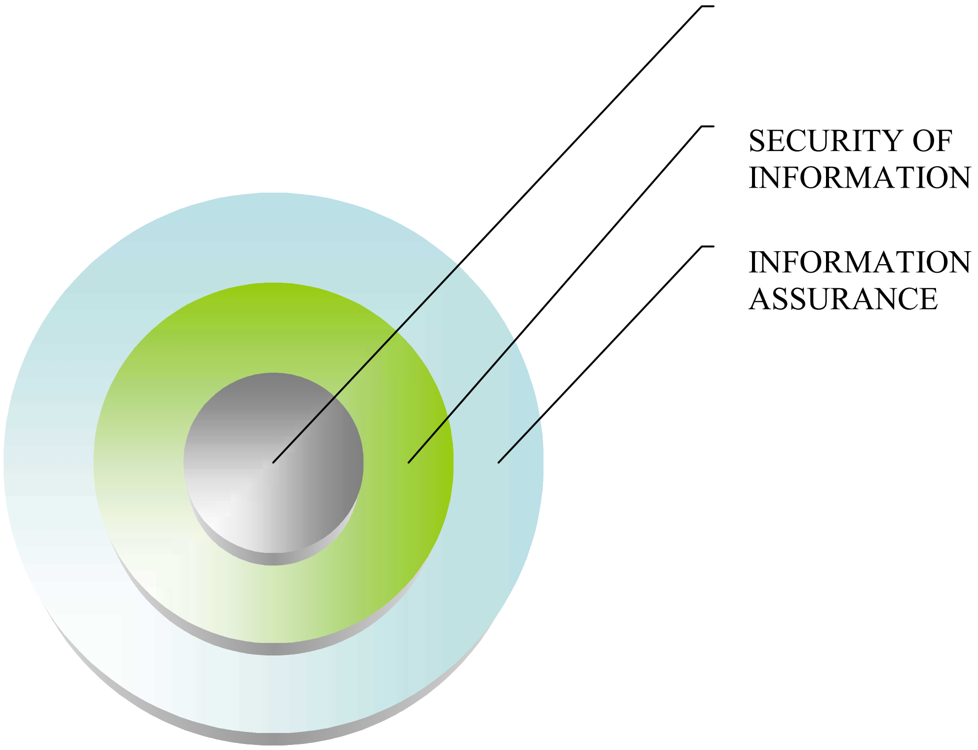


Figure 1: Information security - security of information - information assurance

However, information systems is a comprehensive term that includes all the aspects regarding to infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

2. INFORMATION ASSURANCE AND DATA - INFORMATION - INTELLIGENCE RELATIONSHIP.

Our contemporary humankind is an information society, see the figure 2. There is a strong and discreete relationship between data, information, information assurance, and intelligence within NATO. Intelligence is not only the product resulting from the intelligence cycle but also intelligence generate through the intelligence warfighting function. Intelligence staffs direct collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The keywords of this chapter are: NATO, information, information assurance, intelligence role and cycle.

In chapters two and trhree, we analyze the security of information and the information treats through a NATO military operations approach, especially for explaining the information assurance role in obtaining and preserving the information superiority within the NATO operations.

Figure 2. The informational contemporary humankind

2.1. Information assurance and data - information - intelligence relationship.

In the beginning of this section, it is useful to analyze the key terms that will be used. In respect of this aspect, we will bring in attention the main ideas of this section:

- data – information - information assurance - intelligence relationship;
- the role of intelligence within NATO.

For explaining the meanings of the terms of interest in this chapter, we will use the original AP-6(2007), NATO glossary of terms and definitions.

Intelligence = the product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity.

Intelligence cycle = the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users.

Communication and information systems = collective term for communication systems and information systems.

Area of operations = an operational area defined by a joint commander for land or maritime forces to conduct military activities. Normally, an area of operations does not encompass the entire joint operations area of the joint commander, but is sufficient in size for the joint force component commander to accomplish assigned missions and protect forces.

Joint operations area = a temporary area defined by the Supreme Allied Commander Europe, in which a designated joint commander plans and executes a specific mission at the operational level of war. A joint operations area and its defining parameters, such as time, scope of the mission and geographical area, are contingency - or mission - specific and are normally associated with combined joint task force operations.

Area of intelligence responsibility = an area allocated to a commander, in which he is responsible for the provision of intelligence, within the means at his disposal.

Priority intelligence requirements = those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decision making.

Collection management = in intelligence usage, the process of converting intelligence requirements into collection requirements, establishing, tasking or coordinating with appropriate collection sources or agencies, monitoring results and retasking, as required.

Collection plan = a plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies.

After we very clear defined the specific terms, have to underline the information assurance role in data - information - intelligence relationship. In this respect, we analyze this relationship, and we can easy observe when the intelligence cycle is performed, the information assurance for it is fundamental. In other words, we must protect our information during the intelligence process. Moreover, information assurance must protect the information acquisition too. The intelligence products have to be made available for authorized users in a very secure mode. We can perform superb data and information collection and evaluation processes, we can achieve very clear estimations and interpretations, we can made available excellent deductions for commanders, but if we do not put in place a very strong system for security of information, we will lose everything. Our enemies always looking for the breaches and gaps in our security of information systems. In this sense, a strong information assurance is the basic element for protecting our own information. As we stated earlier, ***information assurance is an information operation that protect and defend information and information systems*** by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. And the ***information system is the entire infrastructure, organization, personnel,***

and components that collect, process, store, transmit, display, disseminate, and act on information. **In other words, information assurance is a very important information operation that is performed to protect the information systems.**

Within NATO, the intelligence process[30] is indicated in the figure 3.

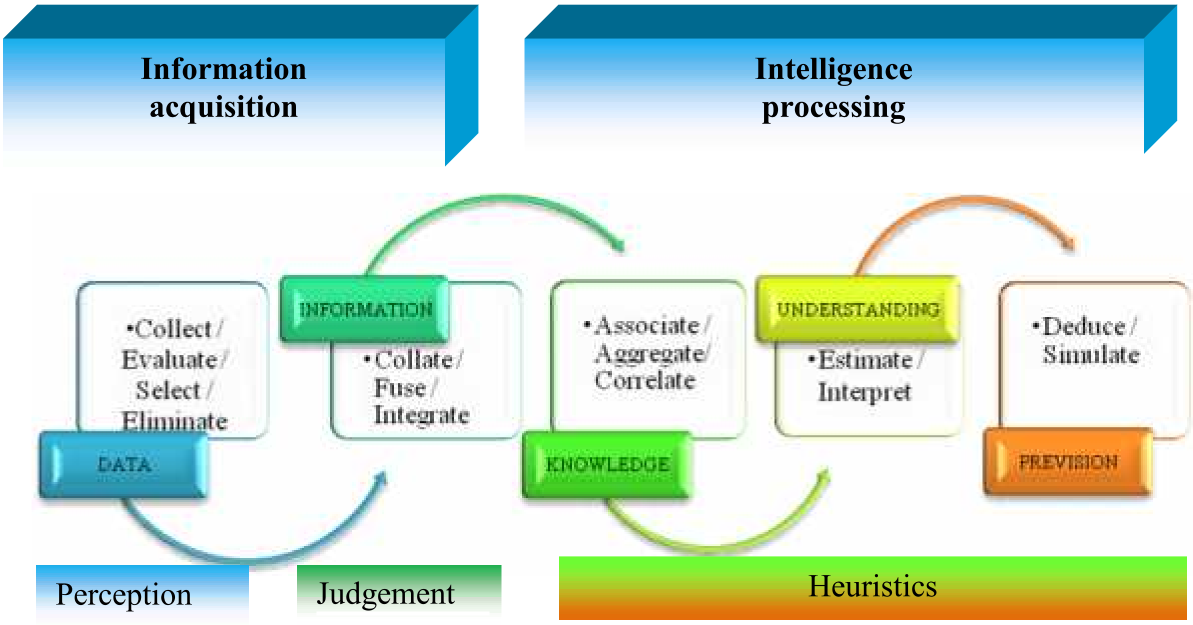


Figure 3: Intelligence process within NATO

Within US Army doctrines[31], the relationship of data, information, and intelligence is described in the figure 4.

The transformation process of the data into intelligence is similar to the NATO intelligence process.

[30] Joachim Biermann, LtCol Louis de Chantal, Reinert Korsnes, Jean Rohmer, Çagatay Ündeger, From unstructured to structured information in military intelligence - some steps to improve information fusion,

SCI, 158-Paper-No3-FinalVersion.PDF, 10.1.6.2.7215[1].pdf), 3-5.

[31] JP 2-0, Joint Intelligence, (2007), I-2.

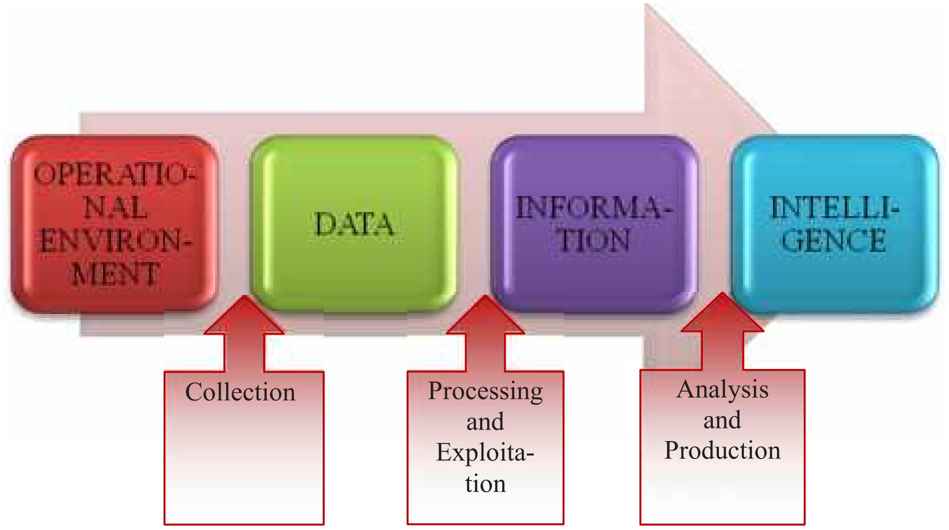


Figure 4: Relationship of data, information, and intelligence within US Army

In the Romanian Army doctrines[32], information product process (see the figure 5) is sensible the same with the previous two.

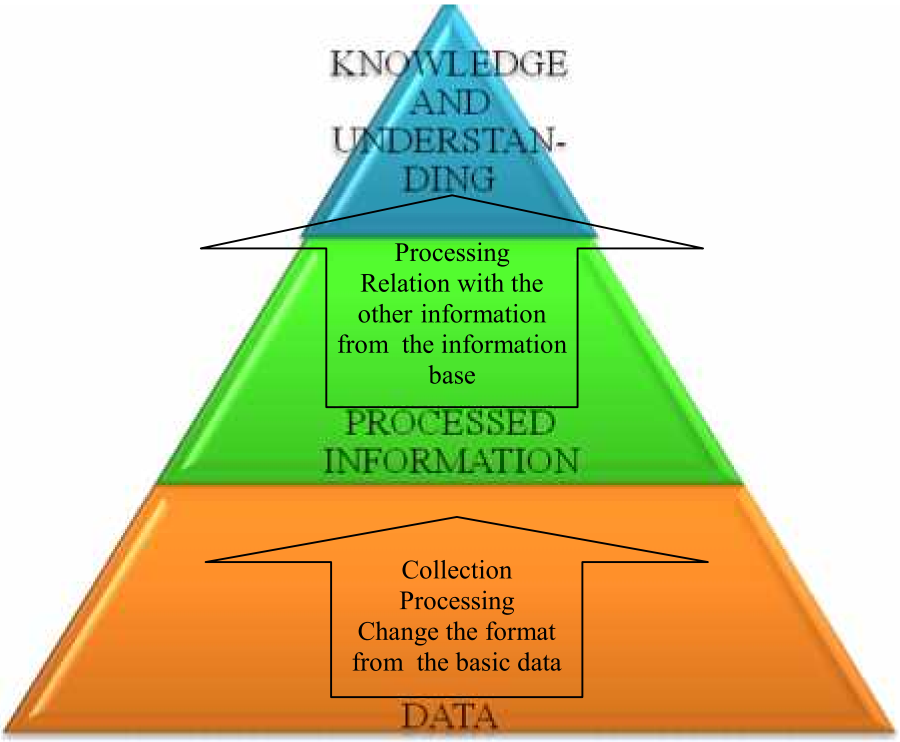

KNOWLEDGE AND UNDERSTAN-DING
Processing Relation with the other information from the information base
PROCESSED INFORMATION
Collection Processing Change the format from the basic data
DATA

Figure 5: Information producing process within Romanian Army

We can observe that all these three intelligence processes are similar. The flows for transforming data into intelligence are almost the same. The most significant differences are encompassed into

[32] IPS-3, Doctrine for information, counterinformation and Army security, Bucharest, (2005), 18.

the particular methods which operate inside of every steps of the intelligence cycle. However, these methodes are much influenced by the proportion between intelligence forces and available resources. An honest collection, coordination and intelligence requirement management (CCIRM) process that is conducted by intelligence staff (which establishes the priority intelligence requests based upon the commander's critical information request and other senior users operational requests) will save this situation.

Within Romanian military doctrines, an approximate translation for ”intelligence” term is ”information”. According to our opinion, ”information” term is similar but not the same with ”intelligence”, the second one being more comprehensive than the previous one. More exactly, is not only a matter of language diferences, but also a different approach of these two terms. First, this is one of the reason that we can not “normally” use in the Romanian language the word ”intelligence” (if we want to express the diferences, we will use the english word ”intelligence”, stressing the quotation marks), because we do not have this word in our national language dictionaries. At the same time, it is clear that these two terms have not the same meaning according to the Allied military doctrines. We can observe this aspect in the definitions indicated in the begining of this article.

On the other hand, we have to underline that another approach can be formulated when we analyze the difference between the ”intelligence” and ”information” terms. We must add that we will analyze ”relevant information” collocation now. According to command and control Field Manual in US Army[33], when the command and control (C2) battlefield operating system is analyzed, an important idea have to be indicated[34]: information is an important aspect of control. Within command and control, *”control”* contribute to accomplish the mission in accordance with the commander's intent. It includes collecting, processing, displaying, storing, and disseminating relevant information for creating the common operational picture (COP), and using information, mainly by the staff, during the operations process. Success in command is impossible without control. The basic elements of control are information, communication and structure. Control allows commanders to set their commander's intent and to adjust their operations acording to the permanent operational situation changes and to the enemy actions. It allows commanders to identify decisive points requiring new decisions during preparation and execution the military operations.

[33] FM 6-0, Mission command; Command and Control of Army Forces, (2006), articles 1-15 to 1-22.

[34] Ibidem.

Generally, information is the meaning humans assign to data. Information is the most important element of control and is divided in two categories: relevant information and execution information.

Relevant information is all information that are important to the commander and staff for command and control. These are the commander's most important C2 resource. Intelligence is an important and distinct subset of relevant information. Information (including intelligence produces) from all echelons generates the COP. All users will share it. By applying proper judgment to the COP, commanders achieve situational understanding and make decisions. Situational understanding will be achieved by the commanders applying analysis and judgment to the COP in order to determine the relationships among the factors of METT-TC[35] (mission, enemy, terrain and weather, troops and support available, time available, civil considerations). METT-TC factors analyze is an important tool that facilitates military decision making process (MDMP) by identifying opportunities for mission accomplishment, threats to mission accomplishment and the force, and gaps in information. At the same time the commander uses his situational understanding for COP, he tries to affect the situational understanding of the enemy (limiting its quantity or quality) and tries to influence the perceptions and actions of others (public or private organizations that influence the success of his operation)[36]. These considerations directly relate to information operations.

According to the Romanian military experts[37], the intelligence concept means relevant information that are processed for exhaustive understanding of operational environment, enemy actions and intentions, and for generating the common operational picture.

Execution information are the information that communicates a higher echelon commander's decision to the subordinate commanders and directs actions, conducts, or procedures. Execution information are orders and plans. In the process, they receive feedback from subordinates and supporting forces. This information flow creates right relations between commander and their subordinate forces, not only by using the feedback but also by using the evaluation of effective actions that are occured in area of operation (AO). This is the main reason that we will use in this paper, the feedback and evaluation like distinct steps within intelligence cycle (the action of feedback and evaluation steps will not be only ceaseless performed but also applied over the all

[35] FM 3-0, Operations, (2008), 1-9.

[36] FM 6-0, Mission command; Command and Control of Army Forces, (2006), articles 1-15 to 1-22.

[37] Constantin Alexandrescu, Gelu Alexandrescu and Gheorghe Boaru, Military Information Systems, (Bucharest: National Defence University "Carol I", 2010), 25.

of fourth main steps of intelligence cycle: direction, collection, processing and dissemination of intelligence produces). In this situation, we can infer that the relationship between data-information-intelligence is a discret relationship one (see the figure 6).

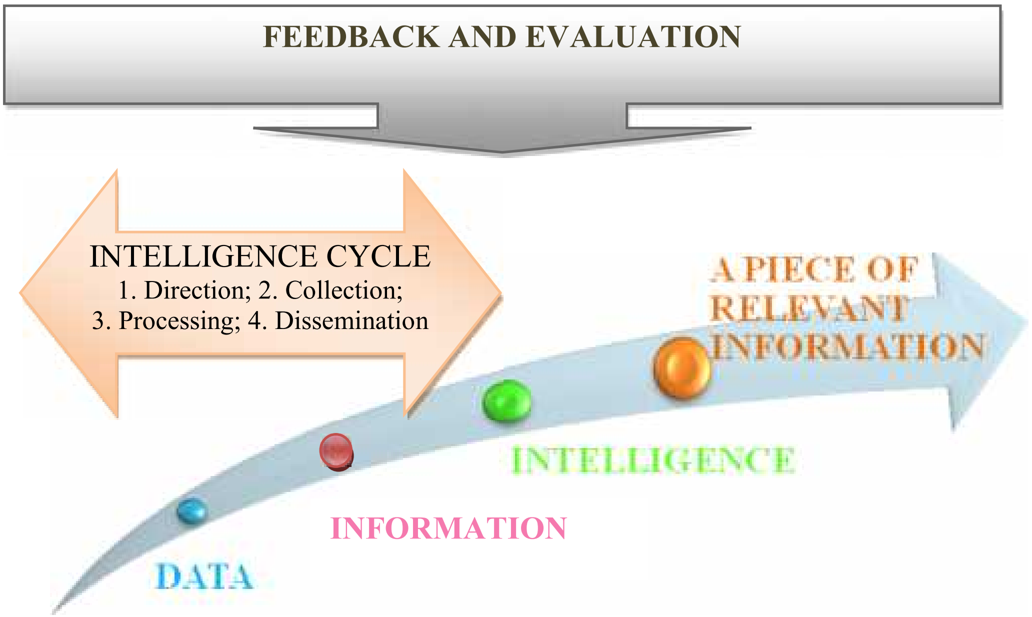


Figure 6: Non discrete relationship between intelligence and relevant information

In this point of the paper, we can observe that:

a. the intelligence processes that was analyzed above have the same main steps to transform data in knowledge and understanding; only the specific methods for performing intellygence cycle will have some particularities;

b. the situational awareness of the battlespace is essential prior to all decisions and activities; the intelligence is essential for it;

c. the relevant and execute information are over the intelligence pyramid. Intelligence process is important when it is finalized with very acurate, continuous intelligence estimates, current intelligence estimates and intelligence summaries;

d. during the operations, a wide variety of information produced by the full spectrum of sensors and human sources has to be collected, filtered, processed and disseminated; an proper, secured, efficient and viable communication and information system is required.

e. strong information assurance operations have to be performed for protecting the intelligence cycle.

Intelligence processing is an important part of command and control because a most accurate situational awareness of the battlespace is essential prior to all decisions and activities. This is done in a structured and systematic series of operations which is called the Intelligence Cycle (the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users). It includes four phases[38] which are defined by the NATO Glossary of Terms and Definitions (AAP-6) as follows:

a. Direction - determination of intelligence requirements, planning the collection effort, issuance of orders and requests to collection agencies and maintenance of a continuous check on the productivity of such agencies.
b. Collection - the exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence.
c. Processing - the conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation.
d. Dissemination - the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it.

These four intelligence cycle phases generate finished intelligence produces to the authorized users. Intelligence requires constant updating in order to remain relevant for users' needs. During the information flow, which is processed and disseminated as intelligence, the operations/phases will overlap and coincide so that they will be concurrently and continuously rather than sequentially; this is the discrete treat of the intelligence cycle. The intelligence products must be secured during a very strong information assurance operation.

Intelligence cycle will permit commanders a full understanding of the operational environment and a proactive approach of militay operations (more active, effective than reactive). In the third and fourth phases of the intelligence cycle information assurance have to be enhanced by not only the security personnel, but also the entire personnel within CJTF.

Concluding this paragraph, regarding to the relationship between data – nformation –information assurance - intelligence and the comparison betwen transformation process of data into knowledge & understanding with intelligence like warfighting function, we can underline two separate aspects:

- intelligence is a very important process during the preparation and execution the NATO operations, for military decision making process (MDMP). This process has a cycle which includes four phases: direction, collection, processing and disemination intelligence products to the commanders, staffs and other users; other two phases are permanently performed: evaluation and feedback;

[38] AAP-6(2007), NATO glossary of terms and definitions (english and french), (2007), 2-I-6.

- in the same time, intelligence is an important warfighting function that provides for the allied comanders an important instrument to apply the combat power of their military structures in the right moment and on the right place;
- information assurance for intelligence cycle must be performed in order to diseminate the intelligence products ***only to authorized personnel in a very secure mode.***

2.2. The role of intelligence and information assurance within NATO

In the second part of this chapter, we will analyze the information assurance and intelligence role during the NATO military operations. We have to stress that, for a better approach, we will analyze the purpose of the intelligence in two Allied doctrines (AJP-01 and AJP-03):

- ***according to AJP-03 (Allied Joint Operations),*** the purpose of intelligence[39] within NATO is to support the planning, execution and support of military operations by provision of timely, tailored and accurate intelligence in accordance with the commanders mission;
- the Joint Force Commander (JFC) will be allocated an area of intelligence responsibility (AOIR) for the conduct of intelligence;
- the intelligence staff based on the JFC directions, will designate an area of intelligence interest (AOII) which will surround and include the AOIR;
- the intelligence staff is responsible for the provision of accurate, timely and relevant intelligence to meet the JFC's requirements within the joint operations area (JOA) and maintaining situational awareness in the JFC's AOII;
- the intelligence assets have to be deployed early in TO; this is essential for the successful conduct of joint operations;
- the deployment of intelligence assets is strongly influenced by the commander's critical information requirements (CCIRs). Priority intelligence requirements (PIRs) are developed from CCIRs;
- the collection, coordination and intelligence requirement management (CCIRM) process established by staffs upon the PIRs, will be passed to the appropriate collection sources and agencies. The resulting information is processed into intelligence to meet PIRs and to support the planning and conduct of operations;
- the joint intelligence architecture will provide opportune and relevant intelligence produces. It must follow the evolution of the operation;

[39] AJP-03, Allied Joint Operations, (2002), 1-5.

- the joint intelligence arhitecture have to have an operational framework within the JOA. This framework will provide links to non-military agencies, as well as appropriate access to NATO and national intelligence databases and national intelligence cells (NICs);
- the joint intelligence architecture has to direct a rapid flow of information and intelligence from all available sources within the JOA. Intelligence cycle must provide intelligence produces in a timely manner; it has to provide support not just to the conduct of joint operations, but to military strategic decision-making at higher levels;
- ***according to AJP-01 (Allied Joint Doctrine),*** intelligence collection analysis, dissemination and sharing[40] role will be critical to anticipating and, possibly, preventing or containing conflicts;
- intelligence processes include relations with non-military agencies and with non-traditional sources;
- intelligence will improve the military decision making process and will reduce the time between the awareness and the execution of an operation;
- intelligence must keep the people awared; it does not only expose the facts, analyzes and intelligence produces but also have to provide awareness to commanders, joint staffs and all military and non-military structures which are involved into an proper operation/activity in a specific JOA;
- NATO will continue to be adapted for responding to threats;
- the Alliance will be enhanced with a broad set of intelligence capabilities that enable a better approach to the challenges; military intelligence groups were deployed in direct support of the brigade combat teams in theatre of operations (TO);
- the Alliance structures need to have the agility to adapt to the most demanding challanges in full spectrum of operations;
- NATO experiences in Afghanistan, Kosovo and other operations have confirmed the complexity of contemporary complex crises that are not simple definition or analysis. Today's challenges demand a NATO comprehensive approach. More exactly, according to the comprehensive approach concept, the aspects of interest will be analyzed by the military actors in cooperation with the civil actors, under the coordination and de-confliction of NATO's military and political instruments with

[40] AJP-01 (D), Allied Joint Doctrine, (2010), 2-10.

the other instruments of power. This implies a close cooperation and planning in accordance with the principles and decisions of NATO bodies.

In this point of the paper section, we analyze the information assurance in accordance with the CNSS Instruction No. 4009, 26 April 2010, National Information Assurance (IA) Glossary, the NATO security directives and publications, the US military security directives and the Security Information Management course statements:

- assurance that information is not disclosed to unauthorized persons, processes, or devices in transit or storage (confidentiality);
- knowledge that data hasn't been tampered with (integrity);
- timely, reliable access to data and information services for authorized users (availability);
- resources (countermeasures) to maintain confidentiality, integrity, and availability against threats and vulnerabilities (protection);
- tamper-evident features (countermeasures) with the purpose of revealing and deterring attempts to compromise, modify, penetrate, extract, or substitute information (detection);
- the ability to return to normal operations (correction) Continuity of Operations (Contingency Planning and Disaster Recovery);
- knowledge of who & where the information is coming from as well as the integrity of the data (authentication);
- sender of data with proof of delivery and the recipient with proof of the sender's identity, so neither can later deny having processed the data (nonrepudiation).

Finally, we fully agree the idea that the main effort of the operation is focused initially on intelligence, information assurance and logistics. For mission execution, commanders need early development of an secured intelligence architecture in TO. This thing means deployable information security personnel and resources, military intelligence forces/structures/groups and a flexible approach of the command and control relations. Performing the operations objectives requires the JFC to determine as soon as possible his commanders critical information requirements. The intelligence community has to put in place a robust and versatile intelligence network in designated AO. The security structures must perform very strong information assurance operation for intelligence cycle protection. The JFC will need adequate sustainment capabilities and will have to determine whether the operation can be conducted at all and at what moment. The deployed military intelligence forces/structures/groups have to support the JFC to execute his mission in TO, to accomplish the operation objective and to achieve the operation end state according to higher echellon's commanders intention.

3. INFORMATION ASSURANCE AND INFORMATION SUPERIORITY

In Chapter 3 we emphasized the need for information assurance within the information operations conducted by the Alliance, with an accent on explaining the relationship between information security, intelligence cycle in NATO operations, and the role of information security to achieve and maintain information superiority in NATO.

As we mentioned before, the intelligence cycle is a discrete transformation of data and information into intelligence produces. The intelligence cycle phases will overlap and coincide, so that they will be concurrently and continuously rather than sequentially. The intelligence cycle will decisively direct the commanders military decission making process and operation execution. The intelligence produces have to be predictive, and support the commander in common operational picture understanding of his designated operation area. The intelligence produces will be an important piece of relevant information. A permanent intelligence estimate will be performed during the "plan, prepare, execute" operations cycle. Information assurance will protect all information flows and systems. Information superiority will be powerful influenced by the information assurance operation and the intelligence cycle produces. The information superiotity will decisively determine the success of the joint operations. The keywords of this chapter are: information assurance for intelligence cycle and information superiority,

3.1. Intelligence cycle within NATO operations

In the beginning of this section, it is useful to analyze the key terms that will be used. In respect of this aspect, we will bring in attention the main ideas of this section:

- Information assurance operations;
- inttelligence cycle within NATO operations;
- information superiority in NATO.

For explaining the meanings of the terms of interest, we will use the original AP-6(2007), NATO glossary of terms and definitions and other US joint publications.

Information superiority = the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. See also information operations. (JP 1- 02. Source: JP 3-13)[41].

Information operations = the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and

[41] JP 6-0, Joint Communications System, (2010), GL-9.

operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. Also called IO. (JP 1-02. SOURCE: JP 3-13)[42].

Assurance = measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy (CNSS Instruction No. 4009, 26 April 2010, National Information Assurance - IA Glossary).

Information assurance (IA) = information operation that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Enterprise Risks – Proactive Security[1].pdf from Security Management Information Course by Regional Department of Defense Resources Management Studies).

We approach this section through IA operations, because of the need for security and protection of the information systems. When we analyze the IA of the information systems we have to take in consideration the information flown within a NATO operation. A very clear information flown must be established between authorized users at all level of NATO operations and between these levels.

Within NATO there are three level of operations: strategic, operational and tactic levels (see figure 7). Strategic level of NATO operations is the highest level. At the strategic level, intelligence will be derived from information gatherd by NATO memmbers over the complete spectrum of national and international military, diplomatic, political and economic matters (according to BI-SC-GIS 65-1 Annex G). The operational level includes operational headquarters in the form of joint force commands, which are tasked to provide a joint task force headquarters, when so ordered by SHAPE. Operational "…is the intelligence required in the planning, executing and supporting campaigns and operations by joint headquarters" (according to BI-SC-GIS 65-1 Annex G). And the tactical level, represented by the battalions within a brigade, which itself is also a tactical-level organization. Tactical "…is the intelligence required by tactical commanders for the planning and conduct of operations, from the level of formations headquarters downwards and produced within the formation's area" (according to BI-SC-GIS 65, Annex G).

The strategic level encompasses both the tactical and the operational, while the operational it looks like a link between the other two. All these three levels will produce intelligence according to the intelligence cycle. This action can be performed during the every level operations

[42] Ibidem.

separately or together. Intelligence is more than just a chart, image or enemy positions on a map. Intelligence must help the joint force commander to understand enemy capabilities and intent.

If Intelligence does not help the commander to understand and to anticipate, if it is not predictive, it is only information, not intelligence*[43]*.

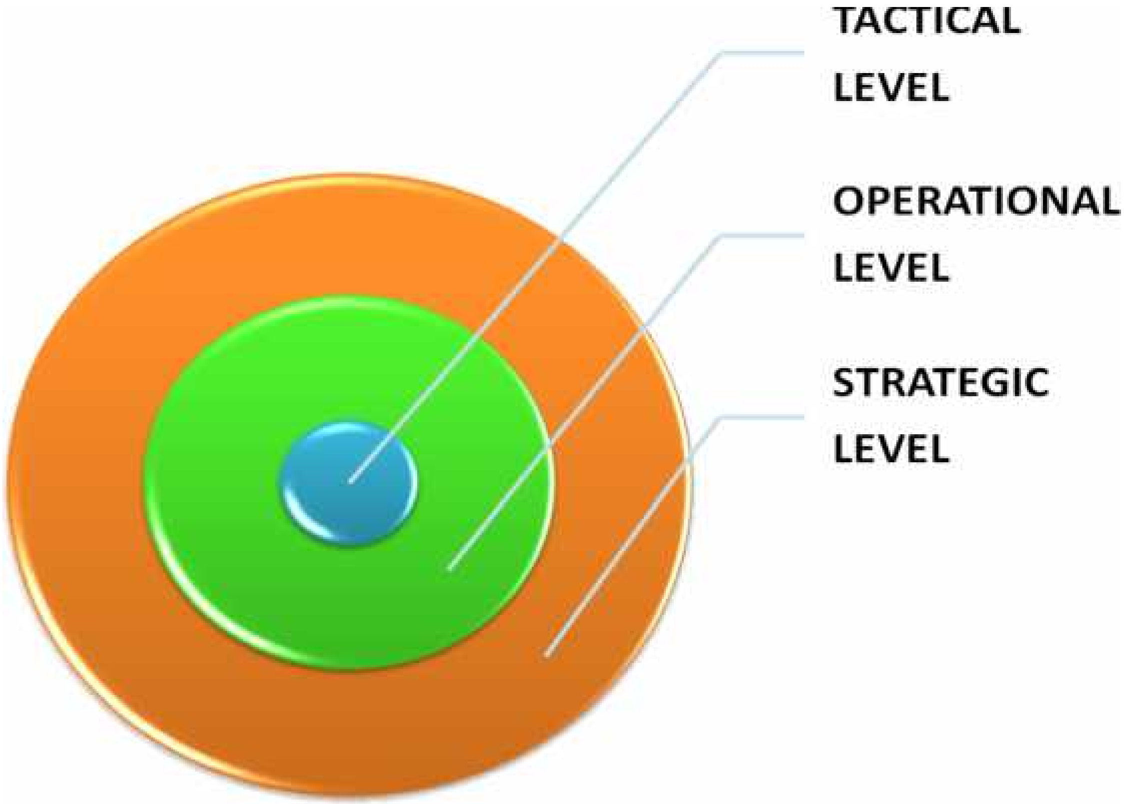


Figure 7: NATO level of operations

Information assurance must protect intelligence cycle, especially the final intelligence products. If in the direction and collection phases, the security of information is more easily accomplished, in the processing phase and, in particular, in the disemination phase of the intelligence cycle, security of information must be very carefully fulfiled. In all intelligence cycle phases, the information systems have to be installed and a very strong security appliance for their protection must be accomplished by the security personnel. But not only the security personnel must be impllied in the security and information assurance of the NATO operation, but also entire militar and non-militar personell which are deployed in an specific theatre of operations.

Within NATO operations, the Intelligence Cycle means the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users (see figure 8).

[43] NATO Intell, PfP ADL-WG, generated from a PfPLMS 0.2 learning object, (2006), 9.

It includes four phases[44] which were defined before in this paper.

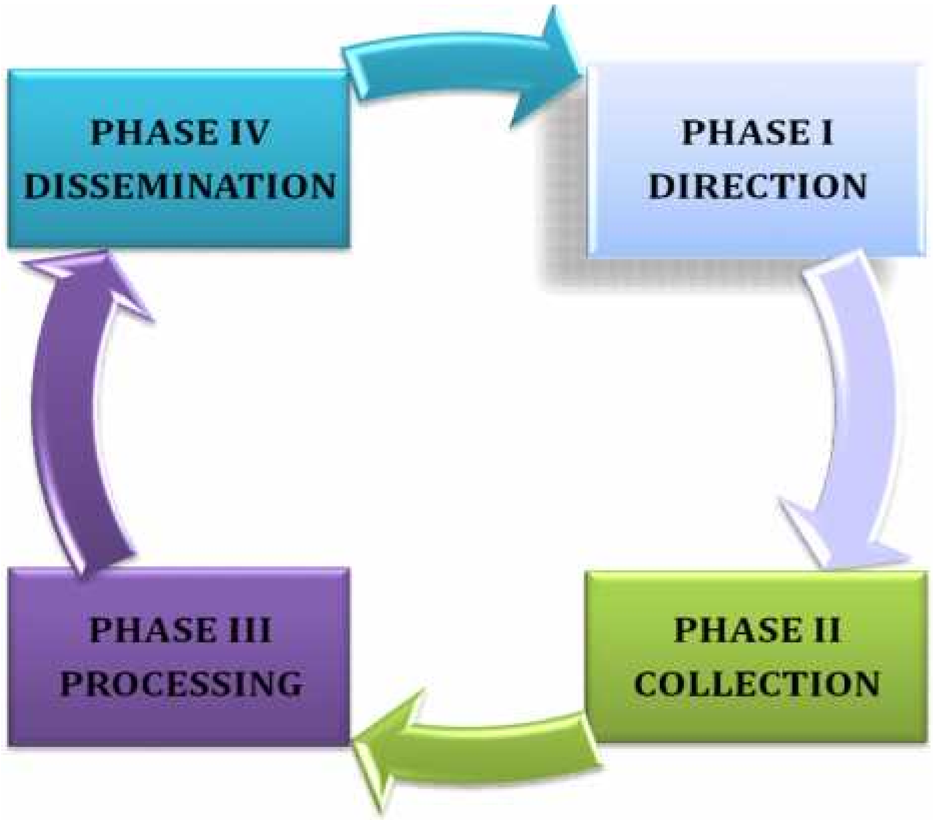


Figure 8: Intelligence cycle within NATO operations

These four intelligence cycle phases[45] generate finished intelligence produces to the users. Intelligence requires constant updating in order to remain relevant for users' needs. During the information flow, which is processed and disseminated as intelligence, the operations/phases will overlap and coincide so that they will be concurrently and continuously rather than sequentially; this is the discrete treat of the intelligence cycle. Intelligence cycle will permit commanders a full understanding of the operational environment and a proactive approach of militay operations (more active, effective than reactive).

The first phase will identify what is relevant for the joint force commander in the specific joint operations area and area of intelligence responsibility. The second, will fill information gaps. The third, will process the information into intelligence. And the fourth, will distribute intelligence to the correct audience, in the correct way, with the correct means and, in a correct

[44] AAP-6(2007), NATO glossary of terms and definitions (english and french), (2007), 2-I-6.

[45] Joachim Biermann, LtCol Louis de Chantal, Reinert Korsnes, Jean Rohmer, Çagatay Ündeger, From unstructured to structured information in military intelligence - some steps to improve information fusion,
SCI, 158-Paper-No3-FinalVersion.PDF, 10.1.6.2.7215[1].pdf), 3-5.

timing[46]. Intelligence cycle is the process by which information is converted into intelligence and made available to users. According to our previous paper, it is very important to realize the clear distinction between information and intelligence. Information is data that has been collected but not further developed. As we have already presented, generally, information is the meaning humans assign to data. Analysis transforms information into intelligence. On the other hand, intelligence is a warfighting fiunction too, and information is an very important important combat power of military structures element and is divided in two categories: relevant information and execution information. In respect of this point of view, we can stress that intelligence is a piece of relevant information.

Both information and intelligence are important, and both may exist together in some form. The base of the intelligence cycle is the mission command. The commander, using a full spectrum operations approach, issues guidance/orientation to his staff. After METT-TC (mission, enemy, terrain and weather, troops and support available, time available, civil considerations) operational variable analysis, the staff will elaborate concept of operations (CONOPS). Now, the coordination and intelligence requirement management (CCIRM) will start. Upon the mission, commanders will elaborate theirs critical commanders information requests (CCIRs). Based on CCIRs, the intelligence staff will establish the Priority Intelligence Requirements (PIRs) and Intelligence Requirements (IRs), to find out the answers to which impact on the CDR's decisions. Keys to successful intelligence support are constant evaluation and feedback from the users and synchronization of the process by the J2/G2. An corect CCIRM process that is conducted by intelligence staff will save many difficult situations during the operation. A common operational picture (COP) will be realized. By applying proper judgment to the COP, commanders achieve situational understanding and make decisions.

The direction phase involves the determination of intelligence requirements. The information flow will be realized by planning the collection effort, monitoring the availability of collection assets, issuing of orders and requests to collection agencies, maintaining a continuous check on the productivity of such agencies and conducting a continuous review of the entire process. The main aspects of this phase are two. First, the intelligence staff has to realize a correct information management and second, the CCIRM must be permanent coordinated by intelligence staff, using the proper and the user's feedback and evaluation.

The commander's requirements direct the intelligence system. All the information, relating to the adversary (threats situation), friendly forces, terrain and weather, and civil considerations, have

[46] NATO Intell, PfP ADL-WG, generated from a PfPLMS 0.2 learning object, (2006), 2.

to be encompassed in a collection plan. These requirements form the CCIRs. From the CCIRs, the J2/G2 develops the commanders PIRs and IRs. PIRs are the requirements that the commander has already anticipated and stated in priority order to aid his decision making process. IRs have to fill a gap in the command's knowledge or understanding of the battle space or threat forces.

The second phase is the collection. It is guided by the commander's IRs and is facilitated by the collection plan. In this phase, information and intelligence will meet the commander's requirements. IRs are then converted into collection requirements and will be passed to the appropriate sources or assets. Collection management will determine what intelligence systems must collect commander’s IRs and will direct how and when to collect its. In the final part of the collection phase, the information collected will be timely delivered to the next intelligence cycle phase where the information will be processed into intelligence.

The third phase of the intelligence cycle is processing. In this phase, five main activities will be performed: collation, evaluation, analyzes integration and interpretation. The information gathered during the collection phase becomes intelligence and targeting data. This analyzed and evaluated information is often verified by other information from other sources. In this manner, "all-source intelligence product" will be made. One of the most important roles of these all-source intelligence products is to provide predictions that will help the commanders during military decision making process and during the operation execution. Upon the collected data, the S2/J2/G2 will elaborate the most probable and the most dangerous enemy course of action (COAs) and will support the targeting process.

The fourth phase of the intelligence cycle is the dissemination. This means that the accurate and relevant information or intelligence, in an appropriate form, and by any suitable means, will be timely distributed to those who need it. An proper, secured, efficient and viable communication and information system is required. Dissemination is conducted by de intelligence staffs to support the planning and execution of operations. The time factor is critical during the intelligence dissemination.

In the end of this section, we have to underline some aspects. The intelligence cycle is an discrete transformation of data and information into intelligence produces. The intelligence cycle phases will overlap and coincide, so that they will be concurrently and continuously rather than sequentially. The intelligence cycle will decisively direct the commanders military decission making process and operation execution. The intelligence produces have to be predictive and support the commander in common operational picture understanding of his designated operation area. The intelligence cycle must be protected by an effective information assurance process. Not only the security personnel is implied in the information assurance process, but also entire military or non-military personnel in the theatre of operation or in generally.

3.2. Information assurance and information superiority within NATO

In the second part of this chapter, we analyze some aspects related to information assurance role in preservation of the information superiority within the national and NATO doctrines.

We have already analyzed before this section, what the information assurance means. Now, we can start the information superiority analyze, and the information assurance - information superiority relationship. In the Romanian doctrine[47], information superiority means the collection, processing and dissemination of an accurate and credible information flow, and to deny the same actions for enemy forces. According to the Romanian military experts[48], the information superiority means relevant information that are processed for exhaustive understanding of operational environment, enemy actions and intentions, and for generating the common operational picture.

Within Allied doctrine[49], information superiority is analyzed inside of allied operations concept. As we can see in the figure 9, information superiority within allied operations is a very complex process which copmprise an information operations strategy established by the designated allied structure inside of Joint Force Command. This allied structure will coordinate special operation, intelligence operations, civil-military cooperation (CIMIC) operations, communication and information systems installation, command and control systems, security operations, deception operations, psychological and electronic warfare operations.

Information superiority, together with air superioriy/supremacy and naval presence before the joint forces engagement in battle are the main aspects of success combined joint task force operation. Information superiority is vital for major losses and damages avoiding. In the same time, improved synchronization among joint and multinational forces is essential for effective command and control during the allied joint force opeations. Information systems and networks provide the predominant source from which the warfighter generates, receives, shares, and utilizes information. The installation of an advanced communications and information system which have to be able to sustain produces dissemination through an certain intelligence

[47] Information support of Joint Operations, (Bucharest, 2003), 58.

[48] Constantin Alexandrescu, Gelu Alexandrescu and Gheorghe Boaru, Military Information Systems, (Bucharest: National Defence University “Carol I”, 2010), 25.

[49] AJP-03, Allied Joint Operations, (2002), 2-22, 4-13.

cycle (properly applied during military decision making process), leads to information superiority, which is essential to success in all military operations.

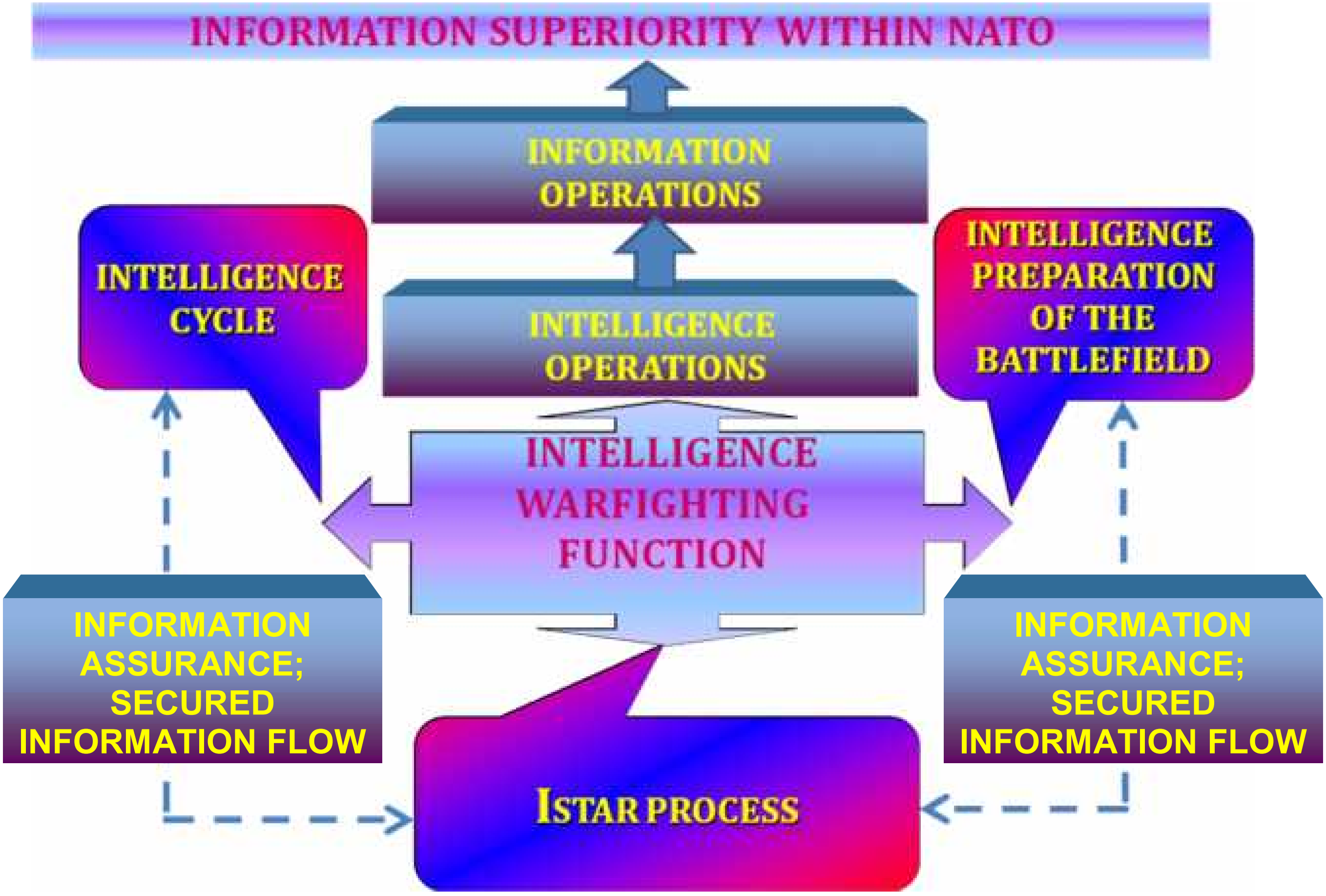

INFORMATION SUPERIORITY WITHIN NATO
INFORMATION OPERATIONS
INTELLIGENCE CYCLE
INTELLIGENCE OPERATIONS
INTELLIGENCE PREPARATION OF THE BATTLEFIELD
INTELLIGENCE WARFIGHTING FUNCTION
INFORMATION ASSURANCE; SECURED INFORMATION FLOW
INFORMATION ASSURANCE; SECURED INFORMATION FLOW
ISTAR PROCESS

Figure 9: Information superiority within NATO

We agree the idea that NATO is dominated by the United States, and NATO intelligence is dominated by US intelligence intentions and procedures[50]. According with this idea, we will analyze information superiority based on the US Army doctrines too.

In the US doctrine[51], there are some provisions about information and information management. Information is a hub of every military activity. In the past, military leaders have recognized that the effective information superiority is a key factor to victory in battle. Information superiority is more than having an edge over an adversary. It is more than just sustaining the information needs of our own forces. It also involves denying an adversary's ability to do the same.

[50] Friedrich W. Korkisch, NATO Gets Better Intelligence, (Viena: Center for Foreign and Defense Policy , 2010), 16.

[51] JP 6-0, Joint Communications System, (2010), I-5.

The power of superiority in the information environment mandates that the joint force commanders fight for it as a first priority even before hostilities begin. This requires higher echelons to develop applicable doctrine, tactics, techniques, and procedures, organizational relationships, and technologies. The quality of information depends upon the accuracy, timeliness, relevance, usability, and completeness of information from all sources. A priority responsibility of command is to ensure access to all relevant information sources within and among all military and non-military organizations which are involved in joint military operations or non-military operations (according to NATO comprehensive approach), and in multinational operations with mission partners. The ***continuous sharing of information*** from a variety of sources facilitates joint force mission execution in a specific area of operation and timelineness awareness for multinational military and non-military structures.

In this point of the paper, we can analyze the new NATO concept: "need to know vs. need to share". We have to underline that there are two ways of approach to this subject. First, it is about the intelligence produces which need to be shared to partners in an area of operation. Second, it is about the necessity of need to know sharing of information, applying all the security measures for the information transferring. Otherwise, the Wikeleaks lesson learned can be repeated.

Within US Army, information superiority requires[52]:

a) seamless architecture and systems integration;
b) responsive information collection, processing, and dissemination;
c) prioritized requirements and assign responsibilities;
d) information operations, (in our opinion, including information assurance).

The information superiority results are:

a) enhanced command and control;
b) recise knowledge of friendly locations;
c) fused all-source intelligence;
d) accurate adversary locations;
e) degraded adversary command and control.

Information must have the following quality criteria:

a) accuracy - information that conveys the true situation;
b) relevance - information that applies to the mission, task, or situation ahead;
c) timeliness - information that is available in time to make decisions;
d) usability - information that is understandable and is in commonly understood format and displays;

[52] JP 6-0, Joint Communcations System, (2010), I-6.

e) completeness of all necessary information required by the decision makers;
f) brevity - information that has only the level of detail required;
g) security - information that has been afforded adequate protection where required.

Now, we can easy observe that information superiority can not be achieved without information operations, in our particular case, without information assurance operations. The security quality criteria of the information must be assured and preserved by the entire personnel during a NATO operation.

In conclusion, we have to stress the importance of information assurance for the intelligence cycle and for information superiority within NATO operations. The intelligence cycle has a discrete architecture and will provide opportune and relevant intelligence produces to the joint force commanders and other authorized users in a specific joint area of operations. The intelligence cycle must follow the evolution of the operation. A permanent intelligence estimate will be performed during the military decission making process and operations execution. Information superiority is one of the most powerful intelligence cycle achievment. It decisively infuenced the success of the joint operation. Information superiority must be preserved and enhanced by the information assurance. Information assurance is an information operation that must be planned by the security military or non-military experts and executed by the entire personnel during the entire intelligence cycle life time.

CONCLUSIONS

In the final of this paper, we can conclude that there is a distinct relationship between security of information, information security and information assurance. Te first term, security of information, is related to information in generally, in other words, security of all types of information. Information security (INFOSEC) is encompassed in security of information term, because it means security of information handled in electronic systems. In other words we can say that INFOSEC is security of electronic information. Both these terms are included in information assurance term, referring to information systems security in generally.

However, information systems is a comprehensive term that includes all the aspects regarding to infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Regarding to the relationship between data - information - information assurance - intelligence and the comparison betwen transformation process of data into knowledge & understanding with intelligence like warfighting function, we can underline two separate aspects:

- intelligence is a very important process during the preparation and execution the NATO operations, for military decision making process (MDMP). This process has a cycle which includes four phases: direction, collection, processing and disemination intelligence products to the commanders, staffs and other users; other two phases are permanently performed: evaluation and feedback;
- in the same time, intelligence is an important warfighting function that provides for the allied comanders an important instrument to apply the combat power of their military structures in the right moment and at the right place;
- information assurance for intelligence cycle must be performed in order to diseminate the intelligence products ***only to authorized personnel in a very secure mode.***

On the other hand, we fully agree the idea that the main effort of the operation is focused initially on intelligence, information assurance and logistics. For mission execution, commanders need early development of an secured intelligence architecture in TO. This thing means deployable information security personnel and resources, military intelligence forces/structures/groups and a flexible approach of the command and control relations. Performing the operations objectives requires the JFC to determine as soon as possible his commanders critical information requirements. The intelligence community has to put in place a robust and versatile intelligence network in designated AO. The security structures must perform very strong information assurance operation for intelligence cycle protection.

In the penultimate paragraph of this conclusions section, we have to underline some aspects. The intelligence cycle is an discrete transformation of data and information into intelligence produces. The intelligence cycle will decisively direct the commanders military decission making process and operation execution. The intelligence produces have to be predictive and support the commander in common operational picture understanding of his designated operation area. The intelligence cycle must be protected by an effective information assurance process. Not only the security personnel is implied in the information assurance process, but also entire military or non-military personnel in the theatre of operations.

In the end of our final paper, we have to stress the importance of information assurance for the intelligence cycle and for information superiority within NATO operations. The intelligence cycle has a discrete architecture and will provide opportune and relevant intelligence produces to the joint force commanders and other authorized users in a specific joint area of operations. The intelligence cycle must follow the evolution of the operation. A permanent intelligence estimate will be performed during the military decission making process and operations execution. Information superiority is one of the most powerful intelligence cycle achievments. It decisively infuenced the success of the joint operation. Information superiority must be preserved and enhanced by the information assurance. Information assurance is an information operation that must be planned by the security military or non-military experts and executed by the entire personnel during the entire intelligence cycle life time and for planning and executing of the NATO joint operations.

REFERENCES

1. AAP-3(H), Procedures for the development, preparation, production and the updating of NATO standardization agreements (STANAGs) and Allied Publications (APs), (2001);
2. AAP-6, NATO glossary of terms and definitions (english and french), (2007);
3. AJP-01 (D), Allied Joint Doctrine, (2010);
4. AJP-03, Allied Joint Operations, (2002);
5. JP 2-0, Joint Intelligence, (2007);
6. JP 6-0, Joint Communications System, (2006);
7. FM 2-0, Intelligence, (2010);
8. FM 3-0, Operations, (2008);
9. FM 5-0 (101-5), Army Planning and Order Production, (2005);
10. FM 6-0, Mission command: Command and control, (2006);
11. IPS-3,Doctrine for information, counterinformation and Army security, (Bucharest: 2005);
12. Information support for Joint operations doctrine, (Bucharest, 2003);
13. FT-2, Operation doctrine for Army, (Bucharest: 2002);
14. Constantin Alexandrescu, Gelu Alexandrescu and Gheorghe Boaru, Information Systems-theoretical-,(Bucharest, National Defence University“Carol I” Edition, 2009);
15. Constantin Alexandrescu, Gelu Alexandrescu and Gheorghe Boaru, Military Information Systems-services and technology-,(Bucharest, National Defence University “Carol I” Edition, 2010);
16. Joachim Biermann, LtCol Louis de Chantal, Reinert Korsnes, Jean Rohmer, Çagatay Ündeger, From unstructured to structured information in military intelligence – some steps to improve information fusion, SCI-158-Paper-No3-FinalVersion.PDF, 10.1.6.2.7215[1].pdf;
17. Friedrich W. Korkisch-NATO Gets Better Intelligence, Center for Foreign and Defense Policy, Viena, 2010.
18. NATO Intell, PfP ADL-WG, generated from a PfPLMS 0.2 learning object, (2006).

19. Security within the North Atlantic Treaty Organization, C-M(2002)49 dated 17 June 2002, http://www.statewatch.org/news/2006/sep/nato-sec-classifications.pdf .

20. Corrigendum to C-M(2002)49 Security within the North Atlantic Treaty Organization, C-M (2002)49 dated 17 June 2002dated, Amendment 7, http://www.nbu.cz/_downloads/pravni-predpisy---nato/container-nodeid-751/c-m200249-cor3-nu-pd-security-within-the-north-atlantic-.pdf .

21. CNSS Instruction No. 4009, 26 April 2010, National Information Assurance (IA) Glossary, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf .

22. Department of Defense Dictionary of Military and Associated Terms, 2001, amended through 2003, p.255.

23. AC/35-D/2002-REV2, Appendix 6, Annex 1, http://www.nbf.hu/anyagok/jogszabaly/AC_35-D_2002-REV2.pdf .

24. The NATO Programme for Security through Science, Information and Communications Security: Information and Communications Security Supporting cooperation on information systems and communications networks, http://www.nato.int/science/publication/pdf/ics_en.pdf .

25. NATO Individual Fellowship 1999/2001 Final Report Strategic and Organisational Implications for Euro-Atlantic Security of Information Operations Dr Andrew Rathmell RAND Europe (www.randeurope.org) & Information Assurance Advisory Council (www.iaac.org.uk) http://www.nato.int/acad/fellow/99-01/rathmell.pdf .

26. Ministry of Defence, Draft doctrine for Information Operations; Joint Doctrine Pamphlet XX-01. Joint Doctrine and Concepts Centre, Shrivenham, 1 March 2001.

27. http://www.jrc.deppy.it .

28. G8 Government/Industry Conference on High-Tech Crime, Report of Workshop 3: Threat Assessment and Prevention, Tokyo, 22-24 May 2001.

29. AP, “National Security Adviser sees cyberterrorist threat”, 26 March 2001, cited in NATO Individual Fellowship 1999/2001 Final Report Strategic and Organisational Implications for Euro-Atlantic Security of Information Operations Dr Andrew Rathmell RAND Europe (www.randeurope.org) & Information Assurance Advisory Council, (www.iaac.org.uk) http://www.nato.int/acad/fellow/99-01/rathmell.pdf .

30. SANS SysAdmin, Audit, Network, Security, http://www.sans.org/information_security.php .

31. http://en.wikipedia.org/wiki/Information_security .

32. WiseGEEK, clear answers for common questions, http://www.wisegeek.com/ .

IT&C SECURITY AUDIT

MAJ Ionuț-Răzvan CRACIUN

INTRODUCTION

Information is a very important value for an individual or an organization. Therefore it requires appropriate protection. Information security protects information from a wide range of threats.

Information security is achieved by implementing an appropriate set of policies, practices, procedures, organizational structures and software functions. It is important that each organization should be able to identify its own security requirements. The organization must use three main sources: risk assessment, analysis of existing legislation and security. To ensure continuous and effective work in the company a permanent and fair evaluation of IT systems is required; in two words: security audit.

What is a security audit?

The word "audit" means that an organization plans to carry out a formal examination for one or more essential components of the organization. This is a familiar area to most executives: they know that auditors will examine financial records and how these records are used. They may even be familiar with physical security audits. However managers are not likely familiar with information security audits, which is an audit of how the confidentiality, availability and integrity of information are assured within an organization.

An information security audit is one of the best ways to determine an organization's information security without incurring the costs and other damages associated with a security incident. Security audit aims to determine all the vulnerabilities of the system.

You can see the phrase "penetration test" used interchangeably with the term "security audit". It is not the same term. A penetration test (also known as pre-test) is strictly an attempt to find security holes concentrated in a critical resource such as a firewall or Web server. Penetration testers can only look at a service on a network resource. They operate usually from outside the firewall with minimum inside information in order to realistically simulate the means by which a hacker could attack the site.

I. PURPOSE OF AUDIT FOR COMPUTER SYSTEMS

1. Definition. General concepts

To audit the systems means to collect and assess evidence in order to determine whether the computer system is secure, whether it maintains the integrity of the processed and stored data, it allows to the company's strategic objectives to be achieved and whether it uses efficiently information resources.

During an audit of the computer system the most frequent operations are checks, assessments and tests concerning the information facilities, as follows:

- risk identification and assessment within the system;
- evaluating and testing the system control;
- physical review and evaluation of the computing environment;
- review and evaluation of information system management;
- software verification and evaluation;
- review and evaluation of computer network security;
- review and evaluation of recovery plans and procedures in case of disaster and business continuity;
- testing the data integrity.

IT Audit is a broad field that includes all audit activities for: specifications, designs, software, databases, lifecycle processes of a program, computer software, of a management information system and a maximum portal complexity associated with a virtual organization.

In computer science there are several lines of audit development. Auditing software is the activity that highlights the correlation degree between specifications and the developed program.

The database audit is an area of extreme complexity since it usually involves working with databases comprising genuine data accompanied by the relations established between themselves and the programs that help to manage the data.

The audit aims to define those data elements which determine the extent to which stored data meet quality requirements: accuracy, completeness, uniformity, such understanding, temporality, reproducibility.

The IT audit assesses the IT risks or software, such as calculating salaries or billing. These missions are done by choosing the assessment process together with the client.

The IT audit may refer to physical IT security risk assessment, logical security, changes management, assistance plan, etc. In the general case, the IT audit refers to a complex IT process to respond to a specific customer demand.

IT audit may also evaluate strategic aspects or those related to the quality of IT systems.

Therefore, during the IT audit, it is essential to plan and define the audit method. Choosing an inappropriate method leads to inappropriate use of tools and the audit outcomes are approximate.

The audit is, in its complexity, a task where links, the implications generated by the software, application software or IT system between the developer –software company and user – are analysed. Reports must be viewed from a technical, financial and legal standpoint. Technical aspect refers to the internal data, algorithms, results, used resources. The financial aspect concerns the estimated cost of software, application, system and effective cost, the way payments were made. The legal nature aims contractual obligations and IT legislation.

In order to develop an IT audit an audit plan and an audit program are defined. The plan structure and defining the program are standard, comprising some mandatory steps to be followed. The specificity and complexity of software, of computer application or IT system lead to the performance of different details from a general plan to another, that is from an IT audit program to another

An actual IT audit includes analytical procedures, tests, which highlight the differences between what was planned to be achieved and what was achieved.

The audit ends with a report based on a series of checks of interacting modules of programs, and between subsystems.

In general, the audit is described as an independent examination of records and other information in order to form an opinion concerning check system integrity and improvement of recommended checks to limit the risks. The definition contains significant terms as:

- **Review**; auditing involves gathering and assessing factual information from various sources, it is important that the results of audit process (the primary report containing recommendations to improve the system check) to be followed until the valid sources information;
- **Independent,** auditors are not directly involved in auditing function operations or management; their subordination must ensure the free expression of opinions;
- **Records and other data**; the term often includes what are called " audit records ", auditors should refer to information on business processes and systems being reviewed as the complete entry data forms, reports generated by the system and of course, the personnel involved in the conduct or management processes audited business are;
- **Opinions**; auditors provide both objective facts and subjective opinions on a given situation. Although subjective, their opinions are based on interpretation of the facts and are open to discussion. These opinions may not be agreed with totally, but a comprehensive and frank discussion must be developed;
- **Integrity**; term integrity includes completeness, accuracy and reliability, a control system that is only partially effective may be better than nothing, or can give a false sense of security; auditor will consider both ways;
- **Recommendation**; auditors generate recommendations, but they don’t have the authority to implement any suggested changes nor to impose any changes to the

management, improvements are achieved only through process of explanation, justification and persuasion, by explaining risks represented by the weaknesses identified in the IT by the audit and further, by justifying the need for change in the process and / or system and suggesting the need to allocate resources and taking steps manage the risks;

- **Improved controls**; improving the control system means, in general, adding the missing checks, they are very rare cases when the auditors may recommend the removal of controls generally because they are inefficient, destructive or expensive;
- **Limits**; mistakes and errors can be reduced but can not be completely eliminated, a good activity involves minimizing risks related to expenses and preparing for action in the worst case scenario which could produce (planning for disaster mitigation actions);
- **Risk**, that something can be done in one unfavourable direction; formally, risk is the possibility of combining threats caused either by someone with evil intent or through negligence or incompetence acting on system vulnerabilities. Vulnerabilities are the weaknesses of which generally occur because of lack of control in computer systems and operating procedures. Risk appearance can generate, into some IS catastrophic results.

From another point of view IT audit is a mechanism for reviewing the effectiveness of organizations, systems, processes and risks controls. Audits enable management to:

- discover what actually happens at a time;
- detect potential problems before it's too late to solve them;
- objectively assess the business situation;
- accept reality and take the knowledge to question, even decisions they are difficult;
- implement corrective actions, changes and improvements there where necessary.

2. Types of audit

The main types of IT audit are:

- Audit of computer operating system, revision control computer systems and networks operating at different levels of for example, network, operating system, application software, database controls logical / procedural controls preventive / detective / corrective etc.

- Audit of IT facilities, including issues like security physical working environment controls, management systems and IT equipment;
- Audit of systems under development, covering one or both issues: (1) project management controls and (2) specifications, development, testing, implementation and operation of technical controls and procedural and technical security controls, including controls on business processes;
- IT management audit, including: review organization structure, strategy, work planning, resource planning, establishing budget, cost control, etc.., in some cases, these issues can be audited by auditors and operational auditors leaving more technological aspects of IT;
- IT audit process, review the processes occurring within IT such as application development, testing, implementation, operations, maintenance, incident management;
- Change management audit, review and planning control changes to systems, networks, applications, processes, facilities, etc.., including configuration management, control code development, through testing, production and product change management organization as a result of ICT;
- Control and information security audit, review controls relating to the confidentiality, integrity and availability systems and data;
- Audit compliance with legality, copyright, compliance with legislation, protection of personal data;
- Audit of disastrous accidents / continuity planning business / disaster recovery, revisions to the proposed measures restoration after a disaster affecting the system and the evaluation of organization deals with risk management;
- IT strategy audit, review various aspects of IT strategy, vision and plans, including relationships with other strategies, visions and plans.

In terms of auditing system audit teams information is classified as follows:

- internal audit, confirming compliance procedures transformation of input data into results - aiming to how new system is implemented is more effective, is accompanied by saving resources;
- external audit includes procedures outlining the computer system behavior, the tests by which we shows how stable, how reliable, maintenance procedures are comprising the control system and which implements all express requirements included in the specifications, in law, regulations and by blocking any attempt to restrict the execution of operations prohibited.

II. AUDIT PLAN

1. Audit consulting team

Audit Plan is established as a list of activities to be executed. Running the activity itself is described as a list of activities. The audit process, rigor and professionalism impose developing comprehensive list, structured strictly on the order of importance or execution.

If details are depth, each activity has correspondence in tasks, reports, persons, however defining the new list.

An auditing system, like any complex task is a team activity. Consulting team includes:

- there is a manager with real experience and qualities field work with people to create the appropriate activities audit requirement to maintain the high rate without compromising the burdens, especially for employment in terms of quality and limits;
- establishing rigorous criteria for selecting team members; audit of a computer system is a project any project for which there is a management, is forming a task team manager;
- subjects achieving teamwork, it is known that work of a team that is four times: first time corresponds to defining the task, the second moment corresponds formulating solutions, the third time is the activity itself to implement practical solutions, and the last time the fourth corresponds to the result of the evaluation team, it is important that the definition problem and in developing solutions, the team members to communicate;
- development of real-time reports, development of real-time reports means, first, conducting records of findings "hot", what was seen in the performance of each activity auditor received a tick in the list; more, to obtain data comparable to communicate with team members on procedures and they shall remain constant throughout use them audit process;
- adopting an auditing standard and using a single methods; in a war is only one strategy, one tactical, and arms is compatible to have a single command, if audit process in a similar way things are, is a standard adopted for auditing computer system, set a method of auditing.

2. List of audit building. Types

Building lists is a complex task, particularly important. The lists must be complete, include all elements of communities. It is true that if the missing elements are added or inserted. Or if they included elements of other communities, they are deleted to get the full list. The lists must be the also correct, that order must correspond to the layout position or importance of the item.

The content of the text that describes or defines a list item should be clear, concise, simple, complete, in succession to generate action logic, with inputs and outputs specified. All they have to impose elimination of those elements in texts generating ambiguities of solutions multiple, thereby transforming an implementation measure in the decision making process followed execution under uncertainty. These lists, business plans, steps of procedure, tables of features, not dogmas. They is the set of rules to follow. There are irregularities, but no deviations changes in rules.

The existence of auditing standards and techniques behind building lists. It is important that such lists are compiled that leaves no interpretations.

Since the result is a formal audit is demonstrate transfer of credibility, all items must comply strict standards and auditing techniques, whereas in case of force majeure, the refers, in turn, in sections where it has been performed auditing activities. Do not run any activities that are not included in standard auditing procedures. If you are running evaluations are first data are collected and processed to calculate indicators of methodologies recognized. If additional components being tested or showing that some new procedures, not included in the standards are higher than those required in addition to those required runs and the new procedures. The results add new results binding, which come to strengthen the results obtained by official procedures. The lists are listed distinction between what is required and for which there rigid procedures and everything is extra. It is not Optional, but the processing required, but soft in terms of beneficial to the audit report. These additional steps are only mandatory for auditors, since they are in support of the audit.

Contain enumerated lists, arranged one after the other, components homogeneous, such as module names, file names, the names of entities parameter name codes associated with messages, reports associated names, passwords, access and evaluation results. Enumerated lists as they are built on computer system design and updates as they run the stages of system computer.

Scrolling lists include steps, activities, operations to be operated in a certain order to achieve a certain objective. Scroll lists are prove to be properly developed when, as the stages running information system development cycle is not required interchange of position or insertion of new elements in the list.

Lists of priorities is a particular form of manifestation of vision of the project manager. The priorities concern the relationship between quality and quantity, ways of developing criteria for selecting team members information system development and establish a position that has quality management information system.

The lists of characteristics is extraction from a variety of characteristics of those whom the project manager deems essential and pursued throughout the system development process computer. The lists of features take into account the destination system computer.

Assessment lists are important both in the development and auditing process, because it creates the premises for conducting first self-evaluation process and then process evaluation. Under normal circumstances there should be no significant differences between self and, respectively, or computer system evaluation components.

III. SECURITY AUDIT

1. Audit specifications

Information system specifications, such a house is foundation system. Therefore the audit should begin with the audit system specifications. Specifications are based on sources such as:

- laws and governmental acts;
- rules for the implementation of official acts;
- the technical documentation and production equipment auxiliary;
- the creation and operation of the company;
- monographs, reports and presentations;
- accounts and wealth;
- programmatic documents: strategies and plans on different terms;
- reports on the dynamic evolution;
- Reports on business connections;
- documents defining image for advertising and marketing;
- documentation on employment;
- documentation on research, market research, social activities.

All comparisons with what specifications should include however, using updated lists of factors lead to the drafting a full audit report. Thereafter, all other stages of audit aimed at product specifications developed on the existing.

2. IT audit system project

Computer system design is based on the specifications. Most projects are divided into subsystems. Whichever method used, regardless of development environment used, only a good projectaims to develop an operational computer system.

Price lists and tables are derived from analysis specifications proceed to study the project. A draft system is developed on several levels.

The first level, with the highest degree of aggregation, identifies subsystems comprising the system.

The second level corresponds to a deeper breakdowns, which distinguish the constituent parts of subsystems and flows have been defined.

The third level contains details of the operations and organization operators.

The fourth level contains sufficiently detailed representations that is the programming specifications.

Audit of the project activity must cross all four levels of detail. The measure establishes the next level is direct result of the detail elements defined in the previous level. If in the previous level are itemized on the elements the following details the current level or have not matched on the previous report as an element of contradiction is in the project.

In developing a project has met a set of rules and auditing process is intended to consider whether the rules were observed.

The first factor is associated with a single variable, because factor is unique.

Secondly, an analytical expression has a single indicator. Two analytical expressions belonging to two different indicators only if the terms are different.

Thirdly, an indicator is evaluated once for a data set. He does not appear to be evaluated with the same set of data and a another component of the project.

Fourth, pooling all data for operating a single criterion. The introduction of several criteria to aggregate data creates favorable conditions increase the risk of redundancy in management computer system that develops in stages.

Fifth, the project includes components aimed at basic operations such as initialization, sorting, re, concatenation, additions, calculations, extraction, retrieval, modification, reads, updates, reorganizations, etc..

Audit of computer system design goes, using indicators from the purely qualitative assessments in the analysis, with a rigorous foundation. Items included in the lists and the differences become visible and quantified. In this way it ensures a high degree of a rigorous process that has long been considered an art, and the product result of an inspiration whose roots come from a different environment.

3. Audit of source texts

A special inspection is it the source text, which is scrolling text step by step, highlighting and evaluating the algorithm steps ability to generate errors. Inspection aims to increase software quality by applying rules checked and not taken into account by programmers who developed the product tested. Programming from specifications where present:

- data entry;
- results;
- computer models;
- sets of test data and results to be obtained.

By inspection, place face to face with the specified components corresponding sequences in the program. It identifies the following situations:

- crowd sequences correspond to the specification text instruction sequences in the source program, the audit records that program achieved the requirements defined in the specifications;
- the set of sequences, some sequences of their corresponding text source, and other such sequences correspond to parts of the program source; means that programmers have developed a product that would achieve all processing functions are described by the specifications;
- column source software crowd sequences appear more sequences that are required by the specifications, there are situations in which programmers infer a number of necessary processing program included in the specifications approach because of problems in the text area specified.

The same situations occur in critical testing.

Audit of the source text aims to analyze how the test data is entered, the procedure worked and especially to establish partial nature or completeness of processing.

The audit determined that the source text are the disadvantages of sources and definitions that are also without giving solutions, ie without generating missing sequences to show how to rewrite the program.

Source texts are formulas that define concrete systems programs, along with file / database or other structures involving data and relations between them.

4. Audit data

Data is stored in files or are systematically managed systems database management, are subject to audit like any other component of the system.

The audit data is a complex process as it concerns those components of the computer system aimed at creating and update files or databases.

Audit of these components allows obtaining a complete picture about the software's ability to contribute to a level as higher quality data.

It is important that auditors have software that analyzes the content data recorded to identify:

- introduced articles doubles;

- consistent of events actually generated at a station operating dates and scheduled events.

Data analysis is one of the most difficult stages whereas the data directly influence the audit, without conditions, quality final results are obtained by a computer system.

To determine which is the quality of the data set are listed attributes, characteristics and quality metrics data quality (consistency, uniformity, completeness, accessibility, accuracy, reliability, translation, objectivity, timeliness, relevance, profitability, etc.).

Data audit objective is to determine the extent to which data entry of a software product meet quality requirements for processed.

The audit data is a complex construction involving specific tasks and ends with an audit report.

Audit data includes:

- procedures used to record data analysis and validation on these procedures;
- determine whether the devices used for making measurements are calibrated and meet the requirements of standards that are working;
- establishment of classes of errors and, within the class of errors specific.

IV. AUDIT REPORT

The audit process is completed with a report that proposals for action to reduce and maintain control of significant risk of new applications. Audit report is a work of summary is based on an analysis of the results of crossing source texts, the Startup programs and the interpretation final results, especially through the interpretation of intermediate results and the tracking program.

The audit report is an essential element of the audit by through which the auditory system as the situation was assessed by the auditors. The audit report shall be communicated to the party audited, the auditors' findings and conclusions. The objectives of the audit report are:

- reassure managers in the computer system immediately after the engagement;
- provide useful recommendations on improving procedures operative control and efficiency;
- provide an official record of audit work and response managers.

Audit report is a text which contains:

- presentation context;
- the result of the audit process;
- final evaluations;
- records of each stage of the audit process.

The audit report contains details on:

- product description;
- establishing conditions of normal use;
- prohibited operations to be carried out using the product;
- functions that are developing normally, indicating inputs, outputs respectively;
- side effects that occur when the entries are complete and fair;
- risks that occur when inputs are incomplete and incorrect;
- how to resume the use of procedures.

The audit report shows that the product is used or product becomes usable if you are running a series of improvements. The quality of the report is how it is constructed components. Text structure is formed step by step answers short clear questions: Who? Why? how? Why? It is imperative that reporting to include sections that address the audit issues gradually for a computer system. The first section includes identifiers for:

- computer system that is subject to audit;
- the basis of the audit process is carried out;
- the presentation team of auditors;
- presentation of information system developers;
- present beneficiary of the audit process.

The second section includes elements for:

- defining the objective;
- establishment of established and accepted methods and techniques;
- structuring the audit process.

The third section defines the audit plan and descriptions contains for:

- steps to be taken;
- the resources allocated to each stage;
- flows that are generated;
- the level of stringency and ways to maintain a constant level;
- communication between the audit team, communication auditors with information system developers, with communication beneficiaries of the audit process.

The fourth section contains details of all sources used as questions for the audit:

- contracts;
- specifications;
- computer system design;
- source texts;
- databases;

- test results performed by the team that developed the system computer;
- process documentation;
- tools used by the team that developed the system computer.

The audit report must be clear, concise, constructive Audit report should be compelling not subject to the comments. It must contain a description of obvious questions or comments not covered by the negotiations. Announced structure should be respected, and the text must be consistent. An assertion must be backed up. It must not nuance, with more so should not be contradicted.

CONCLUSIONS

The audit data is a distinct branch of the audit. Here include techniques and methods of auditing software, computer applications, the traditional systems, modern computer systems, the mobile applications and all applications that use Internet resources.

The higher complexity of processes in society information, information systems requirements require a level of extremely high reliability that only supports the computer audit success.

Information Systems Auditor must be able to assist the management team in determining the size of system and number of staff, business areas are used efficient computer systems, the nature of business, where potential losses fall information system, manual controls and the degree of extension technical complexity.

Audit of information systems is a complex task. A team activities - making the computer system - it corresponds also, all team activity - auditing.

Auditing is required to develop or beneficiary to obtain information that provide confidence in use, ensure that expected results are accurate, complete, exact structure and required obtained in real time.

Audit aims to transfer the certainty and confidence information system established by a positive result by a team auditors, consulting firms belonging to a given authority audits earlier.

The audit of a computer system requires a substantial amount of work as it restores the entire route travelled by the team of filmmakers system and, even more, whereas in the analysis itself with the specifications sources on which they were built.

The immediate impact is the use of information system audit with confidence if the result of the audit provides the confidence. For the team development of the computer system if the test passed the audit, the create conditions conducive to the development of new systems, more complex.

BODIES, REGULATIONS AND STANDARDS ON AUDITING INFORMATION SYSTEMS

ISACA (Information Systems Audit and Control Association)
Web site: http://www.isaca.org
Standarde: SISAS (*Statement of Information Systems Auditing Standards*)
Ghiduri: *Guidelines and Procedures for Audit and Control Professionals*

CobIT *(Control Objectives for Information and related Technology)*
Certificări: CISA (*Certified Information Systems Auditor*)

IFAC (*International Federation of Accountants)*
Web site: http://www.ifac.org
Standarde: ISA (*International Standards of Auditing*)
IAPS *(International Auditing Practice Statements)*
Ghiduri: IITG **(***International Information Technology Guidelines)*
IIA *(Institute of Internal Auditors)*
Web site: http://www.theiia.org
*Standarde: SIAS (*Statements on International Auditing Standards*)*

REFERENCES

Arens, A. A., Loebbecke, J. K., Elder, R. J., Beasley, M. S.: *Audit – o abordare integrală*, Ediția a 8-a, Bucureşti, Editura ARC, 2003

Avram, G.: *Auditul sistemelor informaționale*, Referat teză de doctorat, Bucureşti, ASE, 1997

Avram, G.: *Instrumente de evaluare a sistemelor informaționale economice*, Teză de doctorat, Bucureşti, ASE, 2001

Baron, A. M.: *Tehnici şi metode utilizate în auditul calității software*, Lucrare de disertație, Curs de master: Managementul informatizat al proiectelor, Bucureşti, ASE, Facultatea CSIE, 2004

Brândaş, C.: *Auditul sistemelor informatice de gestiune, note de curs*, Timişoara, Facultatea de Ştiințe Economice, Universitatea de Vest, 2004

Capisizu, S.: *Cerințele auditului informației economice*, Referat doctorat, Bucureşti, ASE, octombrie 2001

Capisizu, S.: *Metode de structurare şi realizare a auditului de date*, Referat doctorat, Bucureşti, ASE, iulie 2002

Cazan, D.: *Validarea modelelor de evaluare a calității sistemelor informatice*, Referat doctorat, Bucureşti, ASE, Facultatea CSIE, 2004

Eben, R. G., Strauss, S. H.: *Software Inspection Process*, Mc Graw Hill Inc, New York, 1998

FIREWALLS AND INTRUSION DETECTION SYSTEMS

LT. Emil MOLDOVAN

INTRODUCTION

With the advent of the Internet to local networks of many interconnected companies and institutions, the issue of data security against unauthorized access has become more acute. Extremely important information is now exposed not only unauthorized access inside the institution, but outside access to virtually any corner of the world. A potential attacker could access data strictly confidential information may change extremely important (money of account) or destroy information that exists in one copy. He must not penetrate inside the institution, just to trick the security systems of "victim". Security systems are varied, the most common being to protect access with username and password. Who wants to access some information has to introduce a specific username and password otherwise be denied access. Often, but this protection is not enough, one can try several passwords, with chances to guess the correct one.

There are systems in blocking access to that username if the password is entered incorrectly a number of times. However, protection is still not very secure, a password can take possession due to neglect by a malicious user who posted it on a notebook, the attack can be launched from any corner of the Internet, without the need for access inside the institution . Some institutions by the very nature of their work need to be connected to the Internet to receive information or to offer information on the Internet (presentation of company products associated with such prices). It therefore requires a more secure solution, an extra protection. Such protection is the so-called "firewall" (n wall against the spread of fire). He achieved a level of protection of fundamental unit of information transfer – package who contains the required destination (a 32-bit number represented which uniquely identifies the destination on the Internet) and source (represented by 32-bit number that identifies the Internet source)

1. AGAINST WHAT WE PROTECT

Threats to the security of computer networks may have the following origins: natural disasters or natural disasters, equipment failures, human mistakes operation or manipulation, fraud. The first three types of threats are accidental, while the latter is intentional.

Computer security several studies estimate that half of the costs of incidents are due to actions deliberately destructive fourth quarter disasters and accidental human errors. The latter can be avoided or, ultimately, a better repaired by the application of security rules (regular data backups, mirrored disks, limiting access rights). The threats caused by deliberate actions, there are two main categories of attacks: passive and active.

Passive attacks - are those in which the intruder passing information see-through channel, without interfering with the flow or content of messages. As a result, traffic analysis is done only by reading the identity of the parties to communicate. Passive attacks are the following features:

- It does not cause damage (do not delete or modify data)
- Violates privacy
- The objective is to "listen "to data exchanged over the network

Active attacks - are those in which the intruder engages in theft or messages, or-in modification, replay, or insertion of false messages. This means that he can delete, delay or modifies messages, can make the insertion of false messages or old. These attacks are serious because it changes the status of computer systems, data communications systems. There are types of active threats:

i. Masquerade - is a type of attack in which an entity claims to be another entity. For example, a user attempts to substitute another in its intention of taking secret information (credit card number, password or key encryption algorithm)

ii. Editing posts - makes the message data to be altered by modification, insertion or deletion.

iii. Refusal of Service - occurs when an entity manages to fulfill its function or it is actions that prevent another entity from performing their functions;

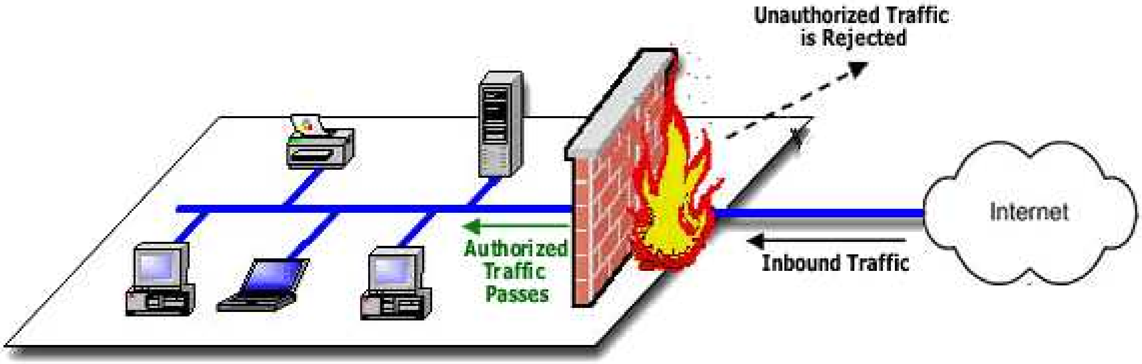
iv. Repudiation service - occurs when an entity refuses to recognize an executive service.

In the case of active attacks be entered some programs created with destructive and that affects, sometimes essential, computer security: viruses, worms, Trojan Horse.

2. WHAT IS FIREWALL?

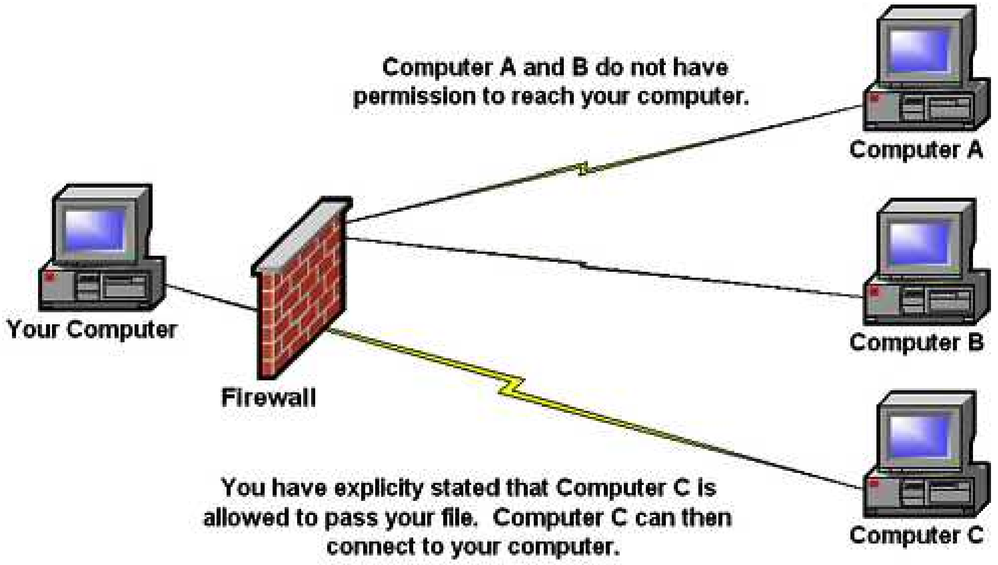
2.1. Introduction

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. In addition, a firewall can prevent participation in an attack against another computer without user knowledge or intention. Using a firewall is especially important if your network or your computer protected at all times connected to the Internet. The most important task of a firewall is to check if a connection is allowed or blocked.



A firewall is a software application or a device that continuously monitors and filters data transmissions made between PC and Internet or local network, to implement a "policy" (methods) filter. This policy could mean:

- protect network resources from any other users of similar networks, all interconnected by wide area network and / or the Internet. Potential attackers are identified, their attacks on local or network PC can be halted.
- control of resources they have access to local users (local network).


Computer A and B do not have permission to reach your computer.
Computer A
Your Computer
Computer B
Firewall
You have explicity stated that Computer C is allowed to pass your file. Computer C can then connect to your computer.
Computer C

Firewall = application that monitors and filters data transmissions made between PC or local network. The firewall prevents strangers to enter your computer through the Internet.

2.2. What "can" and what "can not" do a firewall?

A FIREWALL CAN:

- monitor routes of entry into the private network, thus allowing better monitoring of traffic and therefore easier to detect infiltration attempts;
- block at a time Internet traffic to and from;

- select access to the private space based on the information contained in data packets;
- permit or prohibit access to the public, on certain specified workstations;
- can isolate the private and public space, making the interface between the two.

A FIREWALL MAY NOT:

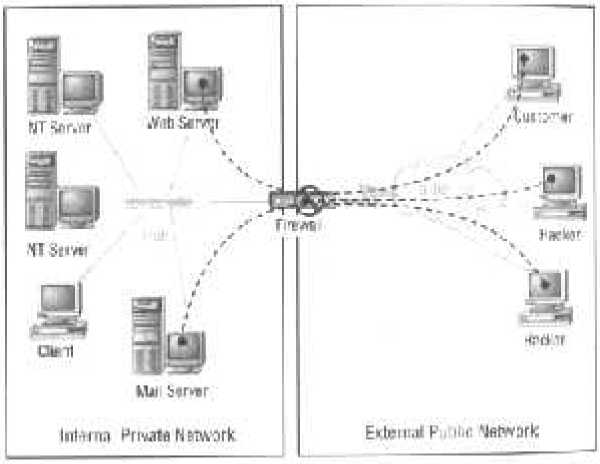
- prohibits the import / export of harmful information circulated as a result of malicious action of operators belonging to the private space (eg, mailbox and attachments);
- prohibit the flow of information on other ways that bypass the firewall (dial-up access that does not pass through the router);
- protect the private network users who use mobile physical systems on the network input device (USB, diskette, CD, etc.).
- prevent the manifestation of the software design faults that run various services and weaknesses arising from the operation of these mistakes.

Therefore, for maximum protection against the dangers of the Internet, in addition to a firewall is needed and other security components.

2.3. Types Of Firewall

Firewalls are devices or software packages that monitor traffic passing through them and accept or block it depending on their rules. They operate at the network layer of security which is one of the oldest and most common type of protection used within security solutions.

Network Firewalls are located as a gateway between the private network and the Internet as shown in the diagram below:



There are three main types of Firewall:

- **Packet Filtering** – Rejects TCP/IP packets from unauthorised hosts and rejects connection attempts to unauthorised services. Packet Filters compare network protocols and transport protocol packets to a database of rules and forward only those packets that conform to the criteria specified in the database of rules. Filters can either be implemented in routers or in the IP stacks of servers.

- **Network Address Translation (NAT)** – Provides security benefits by hiding the actual IP address of a host computer when that host makes a request from servers on the internet. A firewall that uses NAT does this by using its own IP address instead of the hosts when it sends requests to servers out on the internet. When replies come back in the NAT component, the firewall places the hosts real IP address in the packet and forwards it to the host. NAT also has the advantage that only one IP address is needed for a LAN to be connected to the internet.
- **Proxy Services** – Makes high level application connections on behalf of internal hosts to completely break the network layer connection between internal and external hosts. Proxies are application specific and have to be written to support a particular service such as HTTP.

2.4. How to choose a firewall?

First, the decision to implement a firewall should start from a checklist summary of the form:

i. **What are the attacks that I want them block** ? (attacks on TCP / IP operating systems, IP spoofing attacks, DoS attacks (Denial of Service)

ii. **Can I avoid implementation ?** (If our network is completely isolated and will remain so on indefinitely, you probably do not need any firewall (although even so, there are situations where I need to limit access to a network areas).

iii. **What is the budget you want to assign this acquisition?**

iv. **How can justify the return on investment for this acquisition?** (must be able to explain how this expense management can be seen as an investment, and how long this investment can be recovered)

When we have to choice a firewall, we should know that there are a number of criteria underlying the choice itself. Of course, these criteria differ depending on the desired type of firewall:

- **Criterion 1**: The processing capacity - connections per second / packets per second
- **Criterion 2**: inspection skills - is calculated and state information about connections (new, related, established, invalid)
- **Criterion 3**: management tools, logging and reporting - We want to see what happens with our traffic, we want to understand what kind of attacks are directed against us, we want to know when, how, where and why the company was an anomaly in traffic.

- **Criterion 4**: the solution's integration capabilities – It happens that the firewall is not the first security technology introduced in the organization's network architecture. Is necessary that Firewalling technology to be integrated with reporting systems / existing warning or monitoring systems
- **Criterion 5**: the stability of the solution - No matter how many security features would provide a firewall, if it is unstable itself as technology increases security risks.
- **Criterion 6**: technical support and training - firewall solution that will ensure you have support services such troubleshooting / incident response.

3. INTRUSION DETECTION SYSTEM

3.1. Definition

The Intrusion System (IDS) is traditionally deployed to monitor traffic in vital segments in the network, generating alerts when an intrusion is detected. The importance of the IDS has grown significantly as the industry recognizes that 90 percent of attacks in recent years have exploited application vulnerabilities. The traditional stateful inspection firewall, based largely on matching packet header information against Access Control Lists (ACLs), is ineffective to fend off such attacks. A good IDS, on the other hand, can expose these application layer attacks.

An intrusion detection system (IDS) monitors network traffic for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.

IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. There are IDS that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat.

What is intrusion?

An intrusion is somebody attempting to break into or misuse your system. The word "misuse" is broad, and can reflect something severe as stealing confidential data to something minor such as misusing your email system for Spam.

What is an IDS?

Intrusion Detection Systems help information systems prepared for, and deal with attacks.

They accomplish this by collecting information from a variety of systems and network sources, and then analyzing the information for possible security problems.

Intrusion detection provides the following:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Statistical analysis of activity patterns based on the matching to known attacks
- Abnormal activity analysis
- Operating system audit

3.2. IDS Classification

NIDS

Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network.

HIDS

Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected

Signature Based

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that lag time your IDS would be unable to detect the new threat.

Anomaly Based

An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is “normal” for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.

Passive IDS

A passive IDS simply detects and alerts. When suspicious or malicious traffic is detected an alert is generated and sent to the administrator or user and it is up to them to take action to block the activity or respond in some way.

Reactive IDS

A reactive IDS will not only detect suspicious or malicious traffic and alert the administrator, but will take pre-defined proactive actions to respond to the threat. Typically this means blocking any further network traffic from the source IP address or user.

There is a fine line between a firewall and an IDS. There is also technology called IPS – Intrusion Prevention System. An IPS is essentially a firewall which combines network-level and application-level filtering with a reactive IDS to proactively protect the network. It seems that as time goes on firewalls, IDS and IPS take on more attributes from each other and blur the line even more.

Essentially, your firewall is your first line of perimeter defense. Best practices recommend that your firewall be explicitly configured to DENY all incoming traffic and then you open up holes where necessary. You may need to open up port 80 to host web sites or port 21 to host an FTP file server. Each of these holes may be necessary from one standpoint, but they also represent possible vectors for malicious traffic to enter your network rather than being blocked by the firewall.

That is where your IDS would come in. Whether you implement a NIDS across the entire network or a HIDS on your specific device, the IDS will monitor the inbound and outbound traffic and identify suspicious or malicious traffic which may have somehow bypassed your firewall or it could possibly be originating from inside your network as well.

An IDS can be a great tool for proactively monitoring and protecting your network from malicious activity, however they are also prone to false alarms. With just about any IDS solution you implement you will need to "tune it" once it is first installed. You need the IDS to be properly configured to recognize what is normal traffic on your network vs. what might be malicious traffic and you, or the administrators responsible for responding to IDS alerts, need to understand what the alerts mean and how to effectively respond

3.3 . What Intrusion Detection System CAN and CAN NOT provide

The IDS however is not an answer to all your Security related problems. You have to know what you CAN, and CAN NOT expect of your IDS. In the following subsections I will try to show a few examples of what an Intrusion Detection Systems are capable of, but each network environment varies and each system needs to be tailored to meet your enterprise environment needs.

The **IDS CAN** provide the following:

- . CAN add a greater degree of integrity to the rest of you infrastructure
- . CAN trace user activity from point of entry to point of impact
- . CAN recognize and report alterations to data
- . CAN automate a task of monitoring the Internet searching for the latest attacks
- . CAN detect when your system is under attack
- . CAN detect errors in your system configuration
- . CAN guide system administrator in the vital step of establishing a policy for your
- computing assets
- . CAN make the security management of your system possible by non-expert staff

The **IDS CAN NOT** provide:

- . CAN NOT compensate for a weak identification and authentication mechanisms
- . CAN NOT conduct investigations of attacks without human intervention
- . CAN NOT compensate for weaknesses in network protocols
- . CAN NOT compensate for problems in the quality or integrity of information the
- system provides
- . CAN NOT analyze all the traffic on a busy network
- . CAN NOT always deal with problems involving packet-level attacks
- . CAN NOT deal with some of the modern network hardware and features

3.4. Different actions IDS

The main methods used to report and block intrusions on N-IDS are:

Reconfigure firewall

Configure the firewall to filter out the IP address of the intruder. However, this still allows the intruder to attack from other addresses. Checkpoint firewall's support a "Suspicious Activity Monitoring Protocol (SAMP)" for configuring firewalls. Checkpoint has their "OPSEC" standard for re-configuring firewalls to block the offending IP address.

Chime

Beep or play a .WAV file. For example, you might hear a recording "You are under attack".

SNMP Trap

Send an SNMP Trap datagram to a management console like HP OpenView, Tivoli, Cabletron Spectrum, etc.

NT Event

Send an event to the WinNT event log.

Syslog

Send an event to the UNIX syslog event system.

Send e-mail

Send e-mail to an administrator to notify of the attack.

Page

Page (using normal pagers) the system administrator.

Log the attack

Save the attack information (timestamp, intruder IP address, victim IP address/port, protocol information).

Save evidence

Save a tracefile of the raw packets for later analysis.

Launch program

Launch a separate program to handle the event.

Terminate the TCP session

Forge a TCP FIN packet to force a connection to terminate.

3.5. Where do I put my IDS?

Although these questions are largely dependent on your environment, we will try to identify the most common places that intrusion detection mechanisms are installed on. the following illustration taken from http://www.iss.net is just an example .Try to imagine your own environment and where would you place the sensors.

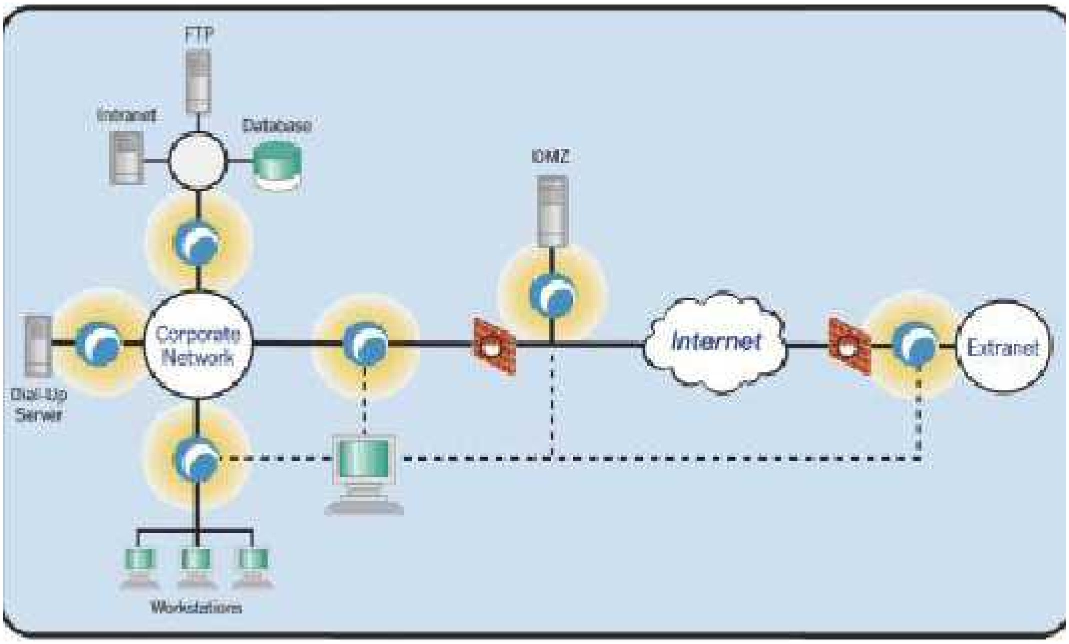


Figure 1. Sensors are represented by round blue dots

As you can see on a figure 1.1 the logical places for the sensors are:

- Between your network and Extranet
- In the DMZ before the Firewall to identify the attacks on your servers in DMZ
- Between the firewall and your network, to identify a threat in case of the firewall penetration
- In the Remote access environment
- If possible between your servers and user community, to identify the attacks from the inside
- On the intranet, ftp, and database environment

The idea is to establish your network perimeter and to identify all possible points of entry to your network. Once found IDS sensors can be put in place and must be configured to report to a central management console. The dedicated administrators would logon to the console and manage the sensors, providing it with a new-updated signature, and reviewing logs. Remember to ask the vendor if the communication between your sensors and management console is secure. You do not want someone to temper the data.

3. 6. My IDS is up, what now?

Once your IDS is up and operational, you must dedicate a person to administer it. Logs must be reviewed, and traffic must be tailored to meet the specific needs of your company. What may look abnormal to your IDS may be perfectly suitable for your environment. You must know that IDS must be maintained and configured. If you feel that you lack knowledgeable staff, get a consultant to help, and train your personnel. Otherwise you will loose a lot of time and money trying to figure out, what is wrong.

Emergency response procedure must exist and comply with your Security Policy. Emergency response procedure must outline:

- Who will be the first point of contact
- List all of the people who will need to be contacted
- Person responsible for decision making on how to proceed in the emergency situation
- Person responsible for investigation of the incident
- Who will handle media, in case the incident gets out
- How will the information about the incident will be handled

4. BENEFIT & LIMITATION

Network-based IDS – Strengths

- Potential lower cost of ownership:
  - All traffic can be monitored with fewer detection points than are needed in host-based system;
  - Management of IDS does not require alterations to host, so unintrusive for end users.
- Detects some attacks that host-based systems miss:
  - IP-based Denial of Service;
  - Malicious Packet or Payload Content (Worms, Viruses,…)
- More difficult for an attacker to remove evidence:
  - Uses live network traffic which can be stored remotely for subsequent analysis/evidence.
- Real-time detection and response
  - Faster notification and response than host-based;
  - Can stop attack before damage is done via automated response, e.g. TCP Reset on connection carrying worm payload.
- Detects unsuccessful attacks and malicious intent
  - Outside a firewall - see attempts blocked by the firewall;
  - Could then refine/update firewall policy.
- Operating system independence
  - Does not require information from the target OS;
  - Does not have to wait until the event is logged;
  - No impact on the target.

Network-based IDS – Weaknesses

- Placement critical in networks:
  - Often place just in front of and/or behind a perimeter firewall;
  - To monitor internal attacks, need sensors at distributed set of potential internal attack points;
  - May need many sensors to get complete coverage of large/complex networks.
- Switched networks make the problem worse: now attack traffic may only appear on one segment.
- Loaded or high-speed networks:

- Number of computations required = #bytes in signature x #bytes in packet x #packets/second x #signatures in IDS database.

Example: signature of 20 bytes x packet size of 300 bytes x 30000 packets/second x 4000 signatures = 720 billion calculations per second!

  - 'Partial recognition' methods as a solution are not reliable – too many false positives.
  - Attacker might be able to flood network to camouflage his real attack.
- IDS may be vulnerable to packet spoofing and fragmentation attacks:
  - Disguise port scanning attack by forging multiple IP source addresses and using source routing;
  - Fragment IP packets forming the attack so they become unrecognisable to the IDS;
  - Does the IDS re-assemble fragmented packets or even an entire TCP connection?
  - If so, does it do so in the same way as the attacked OS does? (Attacker repeats packets with same sequence number – do OS and IDS re-assemble identically?)

Host-based IDS - Strengths

- Verifies success or failure of an attack
  - Was it successful?
  - Log file gives verification.
- Monitors specific system activities, can be tuned:
  - File access activity;
  - Logon/logoff activity;
  - Account changes;
  - Policy changes.
- Detects some attacks that network-based systems may miss
  - Keyboard attacks (wherein attacker walks up to keyboard);
  - File modification, e.g. index.html for web-site defacement;
  - Brute-force login attempts.
- Well-suited for encrypted and switched environments
  - Data is unencrypted at the OS/application level;
  - Can attempt to protect sensitive hosts rather than multiple network segments.
- Potential for near real-time detection and response
  - But generally not as fast as network-based IDS.

- Requires little or no additional hardware
    - Sensors are software only, run on hosts that are to be protected;
    - Though, as with network-based IDS, need additional hardware for console, file storage,…
    - And the IDS may impose a significant overhead on the host.

Host-based IDS - Weaknesses

- Placement critical in networks:
    - Cannot detect attacks on hosts whose log files are not inspected!
- Indirect information
    - Unlike a network-based system, host-based IDS do not monitor attacks directly – rather, they detect the fingerprints left behind by an attacker (if any);
    - Quality of information available in log files varies from system to system: garbage in, garbage out.
- Complete coverage difficult:
    - Need to deploy on every host that is to be protected – possibly thousands in large network;
    - Ensuing cost and management problem.
- Detection may be too late:
    - Outsider has already bypassed network security controls (if any) and may have done damage by the time attack is detected.
    - Unless log files are stored off-host, they may be susceptible to replacement by attacker, thus hiding indicators of attack

5. WHY DO I NEED AN IDS

An intruder normally hacks into your system only after he has carefully accessed you and your security and he attacks you in a systematic way to cause maximum damage. The normal steps towards intrusion are:

Outside reconnaissance: The intruder will find out as much as possible without actually giving himself away. They will do this by finding public information or appearing as a normal user. In this stage, you really can't detect them. The intruder will do a 'whois' lookup to find as much information as possible about your network as registered along with your Domain Name (such as foobar.com. The intruder might walk through your DNS tables (using 'nslookup', 'dig', or other utilities to do domain transfers) to find the names of your machines. The intruder will browse other public information, such as your public web sites and anonymous FTP sites. The intruder might search news articles and press releases about your company.

Inside reconnaissance: The intruder uses more invasive techniques to scan for information, but still doesn't do anything harmful. They might walk through all your web pages and look for CGI scripts (CGI scripts are often easily hacked). They might do a 'ping' sweep in order to see which machines are alive. They might do a UDP/TCP scan/strobe on target machines in order to see what services are available. They'll run utilities like 'rcpinfo', 'showmount', 'snmpwalk', etc. in order to see what's available. At this point, the intruder has done 'normal' activity on the network and has not done anything that can be classified as an intrusion. At this point, a NIDS will be able to tell you that "somebody is checking door handles", but nobody has actually tried to open a door yet.

Exploit: The intruder crosses the line and starts exploiting possible holes in the target machines. The intruder may attempt to compromise a CGI script by sending shell commands in input fields. The intruder might attempt to exploit well-known buffer-overrun holes by sending large amounts of data. The intruder may start checking for login accounts with easily guessable (or empty) passwords. The hacker may go through several stages of exploits. For example, if the hacker was able to access a user account, they will now attempt further exploits in order to get root/admin access.

Foot hold: At this stage, the hacker has successfully gained a foot hold in your network by hacking into a machine. The intruder's main goal is to hide evidence of the attacks (doctoring the audit trail and log files) and make sure they can get back in again. They may install 'toolkits' that give them access, replace existing services with their own Trojan horses that have backdoor passwords, or create their own user accounts. System Integrity Verifiers (SIVs) can often detect an intruder at this point by noting the changed system files. The hacker will then use the system as a stepping stone to other systems, since most networks have fewer defenses from inside attacks.

Profit: The intruder takes advantage of their status to steal confidential data, misuse system resources (i.e. stage attacks at other sites from your site), or deface web pages.

6. DEVELOPMENT

Detection alone is insufficient—it is also important to terminate the attack upon detection. Hence, the trend is to evolve the IDS into an Intrusion Prevention System (IPS), which takes detection to the next level and stops the detected attacks, including application attacks

CONCLUSIONS

As IDS technologies continue to evolve, they will more closely resemble their real-world counterparts. Instead of isolated sensor units, the IDS of the future will consist of sensor units that report to master visualization consoles which are responsible for checking whether alerts from the sensors agree or correlate to likely event-chains. In the future, IDS, firewalls, VPNs, and related security technologies will all come to interoperate to a much higher degree. As IDS data becomes more trustworthy because of better coverage, firewalls and VPN administrators will be more comfortable with reacting based on the input from the IDS. The current generation of IDS (HIDS and NIDS) are quite effective already; as they continue to improve they will become the backbone of the more flexible security systems we expect to see in the not-too-distant future

Hopefully this paper convinced you that IDS is a necessary tool in any environment, and you will take your time to try to persuade your management to implement it. Please remember that deploying IDS requires a lot of research and planing. Once configured correctly it will give you a world of benefit, but if you will neglect to properly configureit, IDS will give you a HUGE headache. Remember that security is not a Patch, which you can implement and forget about. It is a constantly changing concept that if not cared for will lead to disastrous results. Keep yourself constantly updated on the new events.Join web groups, read the news, sign up for alert notifications. If you are a Security Administrator for your company, you can not afford to be left behind, because it will usually mean failure. And failure will usually mean looking for a new job. Then you will never be able to afford that Home Theatre System you always wanted.

REFERENCES

1. Intrusion Detection FAQ , SANS Institute
   http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm.
2. Introduction to Intrusion Detection – ISCA Publications, Prepared by Rebeka Bace -
   http://www.icsa.net/html/communities/ids/White%20paper/Intrusion1.pdf
3. Wikipedia
   http://en.wikipedia.org/wiki/Firewall
4. Virtual Share
   http://vsh.ro/tutorial/326/comodo-firewall/
5. Firewall: frequently asked questions
   http://windows.microsoft.com/en-US/windows-vista/Firewall-frequently-asked-questions

INFORMATION SECURITY IN ORGANIZATIONS

LTC eng. George-Valentin PĂLĂLĂU

I. INTRODUCTION

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities. For this reason, many organizations nowadays implement various security policies in order to protect the organization. Also, to have a secure flow of information, organizations implement an information security framework, which helps the organization to identify the risks associated with the organization's information and ways to mitigate those risks. The challenges for management in providing information security are formidable. Even for relatively small organizations, information system assets are substantial, including databases and files related to personnel, company operation, financial matters, and so on.

II. INFORMATION SECURITY FRAMEWORK

As information security become increasingly important to the continue success for businesses, many are seeking an appropriate security framework. Research on information security management generally addresses two areas: the technical computer security and non-technical aspects [2].

II.1. What is information security management?

Information security management (ISM) is defined as a systematic approach to encompassing people, process and Information Technology (IT) systems that safeguards critical systems and information protecting them from internal and external threats. ISM is increasingly important within organizations, becoming a strategic imperative as security threats continue to escalate. Security and privacy is among the top ten management concerns, according to a 2005 survey of executive IT managers. The absence of a well-defined information policy is currently regarded as the most serious problem with security in organizations today. Navigating the multitude of existing security standards, including dedicated standards for information security and frameworks for controlling the implementation on IT, presents a challenge to organizations. The framework is intended to promote a cohesive approach which considers a process view of information within the context of the organizational operational environment [2].

II.2. What is information security framework?

Information security framework is a comprehensive model that ensures the overall security of information there by eliminating business risks. Information security does not focuses only on technological issue, but also points out other main important elements of an organization such as people, process, business strategies etc., which also mandates the need for information security. The comprehensive information security framework should incorporate the following key elements:

- Recommended sound security governance practices (e.g., organization, policies, etc.);
- Recommended sound security controls practices (e.g., people, process, technology);
- A guide to help reconcile the framework to common and different aspects of generally adopted standards ;
- An analysis of risk or implications for each component of the framework;
- A guide of acceptable options or alternatives and criteria, to aid in tailoring to an organizations operating environment;
- A guide for implementation and monitoring;
- Toolset for organizations to test compliance against the framework.

A comprehensive security framework boils down to three familiar basic components: people, technology, and process. When correctly assembled, the people, technology, and process elements of your information security program work together to secure the environment and remain consistent with your firm's business objectives [2]. **Diagram II.1** shows the concept of people, process and technology.

The information security framework establishes policies and best practices. The framework used for assessing the organization's current information security framework provides a roadmap for the evaluation and improvement of information security policies and practices.

II.3. Significance of information security framework

Diagram II.2 shows the problem organization faces. The company has all the components like software development, polices and procedures, incident management, business continuity management, regulations & audit etc. These components are called islands of security which can't talk each other and also don't work together.

A comprehensive information security framework is the answer for the components to work together, instead of having stand alone components and system. The connected information security framework delivers practical guidance for everyday IT practices and activities, helping users establish and implement reliable, cost-effective IT services. The **Diagram II.3** shows how the information security framework helps different components to interact with one another.

II.4. Tables, symbols, figures, and diagrams:

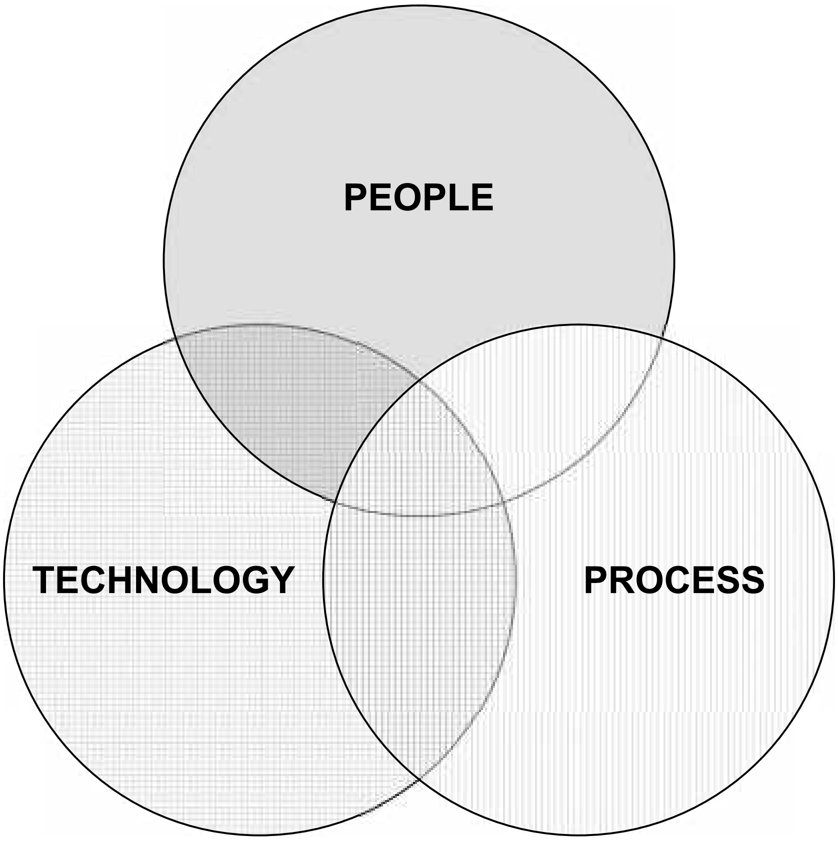


Diagram II.1: *People, Process and Technology* [2]

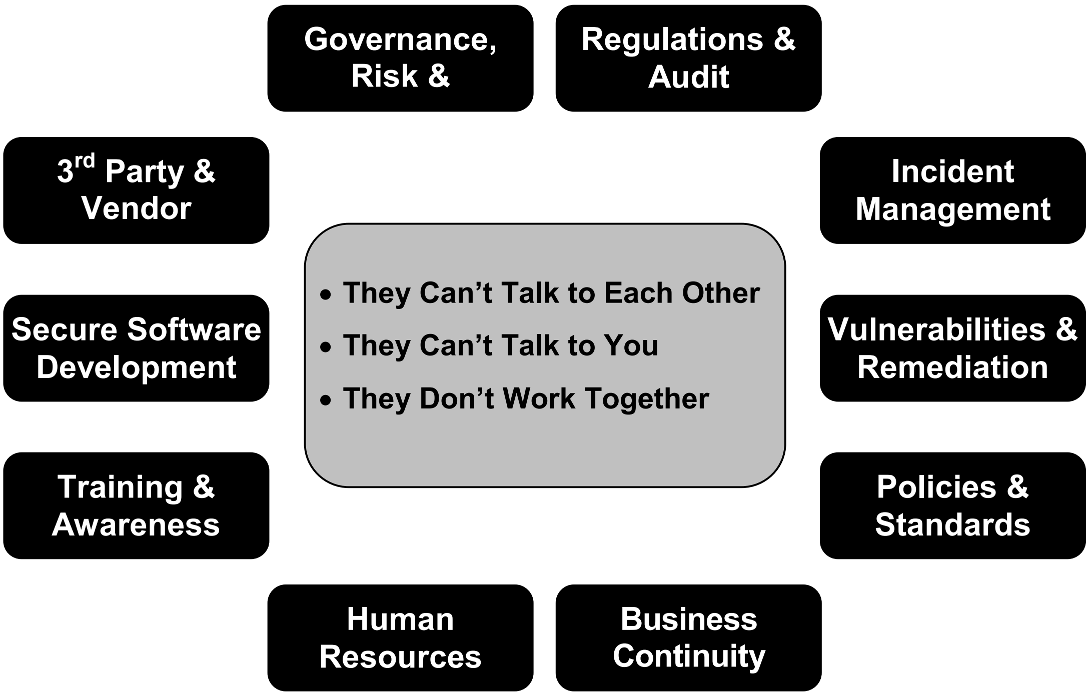


Diagram II.2: *Problem Space* [2]

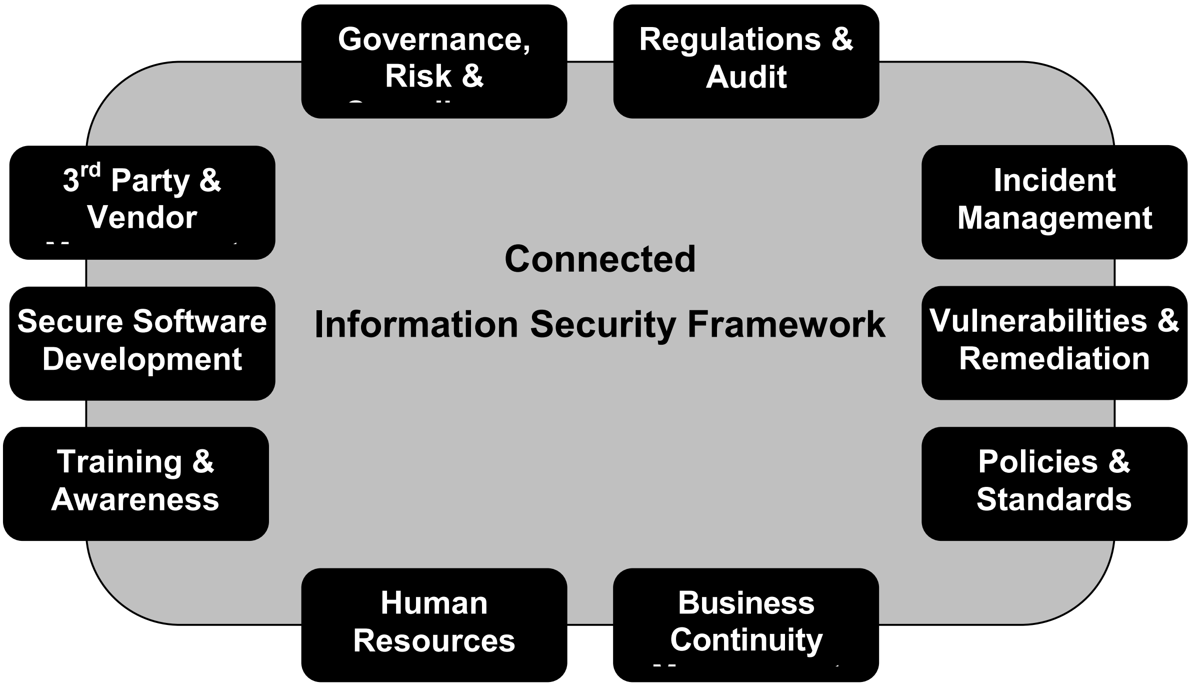


Diagram II.3: *Information Security Framework* [2]

III. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Most of organizations' managers are concerned with issues relating to the management of information security, motivated by the need for cost-efficiency ratio.

Based on the assumption that, in order to achieve cost- efficiency information security, the point of departure must be knowledge about the empirical reality in which the management of information security takes place.

In this respect, there are two main problems relating to information security management:

- What problems do organizations face and what processes do they go through as they are aiming to establish a balanced management system for information security?
- What perceptions do information security managers hold as regards the management of information security in organizations?

III.1. ISMS Background

Too much business security will increase costs and reduce potential revenue streams substantially and it can – in due course – put an end to the business. Conversely, insufficient security might leave the business open for fatal mistakes, espionage, sabotage and crime. The goal of security management in organizations should therefore be to identify and strive toward the optimal point between security and insecurity.

The optimum level of security in an organization (**Figure III.1**), from a strict financial perspective, will be found in the situation were the cost of additional security countermeasures exactly equals the resulting reduction in damages arising from security breaches. This level of security means profit maximization for the organization. Too little security means that security breaches are reducing profits as a result of damages to assets, and too much security means that the costs of security countermeasures consume profits. Hence, we should not strive towards higher and higher security without thinking about the consequences. Moreover, security measures have other consequences than strictly monetary to be taken into account, e.g. social, legal and ethical. Opposing views from various groups of stakeholders to the organization will also have to be recognized [1].

In practice, it is problematical to identify the security equilibrium depicted here. However, in many cases, the total cost of current security countermeasures and the damages arising from current security breaches are not known. And, looking into the future, the potential costs-and-benefits of new countermeasures are even more challenging to estimate. It is difficult to assess the value of a given information asset, since it mainly depends on what it can be used for in the future. As a result, it is problematic to devise economically optimized information security measures [1].

It is widely agreed that organizations in reality do not behave strictly according to a profit-maximizing economic model (as that in **Figure III.1**). Instead, decisions and behaviour are characterized by, at best, bounded rationality and trying to satisfy objectives rather then reaching them [1].

Despite the difficulties outlined above, organizations need to at least try to estimate:

a) the current level of information security;

b) the ideal level of information security; and

c) how to get from a) to b).

III.2. ISMS process model

Any organization that wants to work systematically with information security will need to go through certain stages in pursuit of the goal of optimized information security. In essence, these resemble the common analytical stages known from almost any type of ideal organizational.

The international standard for information security management - ISO/IEC 27001:2005 - defines a set of information security management requirements. It requires that the organization has balanced its information security management system to counter the threats its information assets face. This standard adopts the "Plan-Do-Check-Act" (PDCA) process model, which is applied to structure all ISMS processes. **Figure III.2** illustrates how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meets those requirements and expectations.

Plan-Do-Check-Act (PDCA) is a continuous improvement cycle developed by Walter Shewhart at Western Electric and popularized by Dr. W. Edwards Deming. The four phases - plan, do, check and act - incorporate careful planning with “doing” in small doses, and using feedback to standardize the most effective method:

- **Planning** involves setting boundaries, deciding what data is needed, how it will be collected and what it means. This phase requires an analysis and selection of alternative improvements.
- **Do** consists of carrying out the planned change.
- **Checking** assesses the results of the change.
- **Act** places the most effective alternative as the standard mode of operation.

Then, the cycle starts again with a new set of planned improvements. If the experiment was not successful, skip the Act stage and go back to the Plan stage to come up with some new ideas for solving the problem and go through the cycle again.

III.3. Tables, symbols, figures, and diagrams

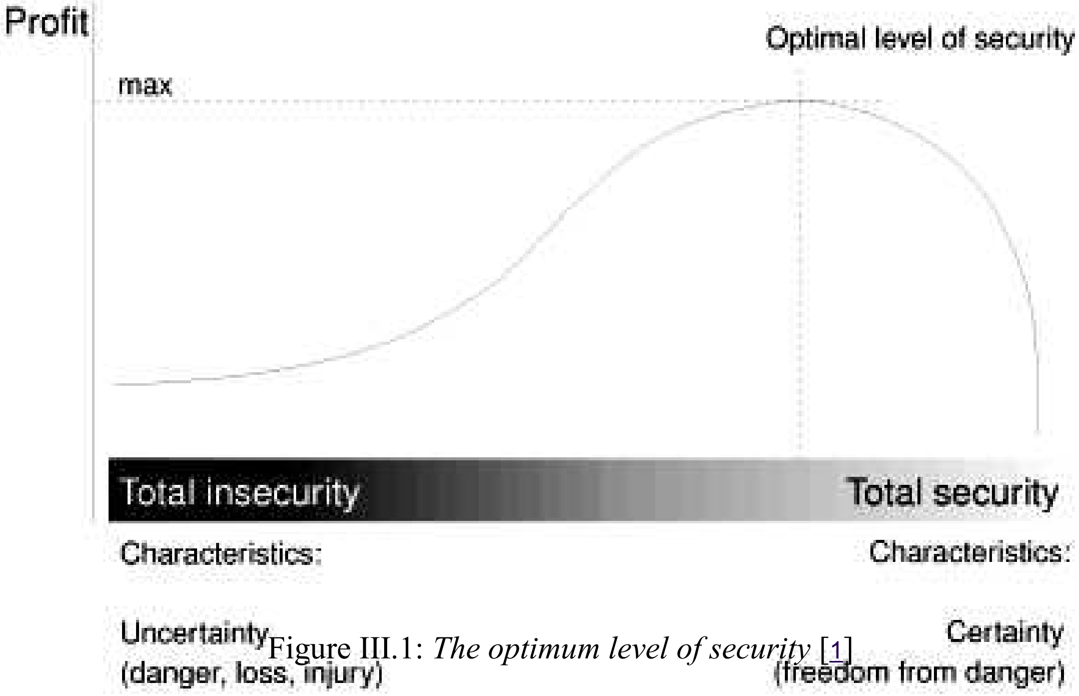


Figure III.1: *The optimum level of security* [1]

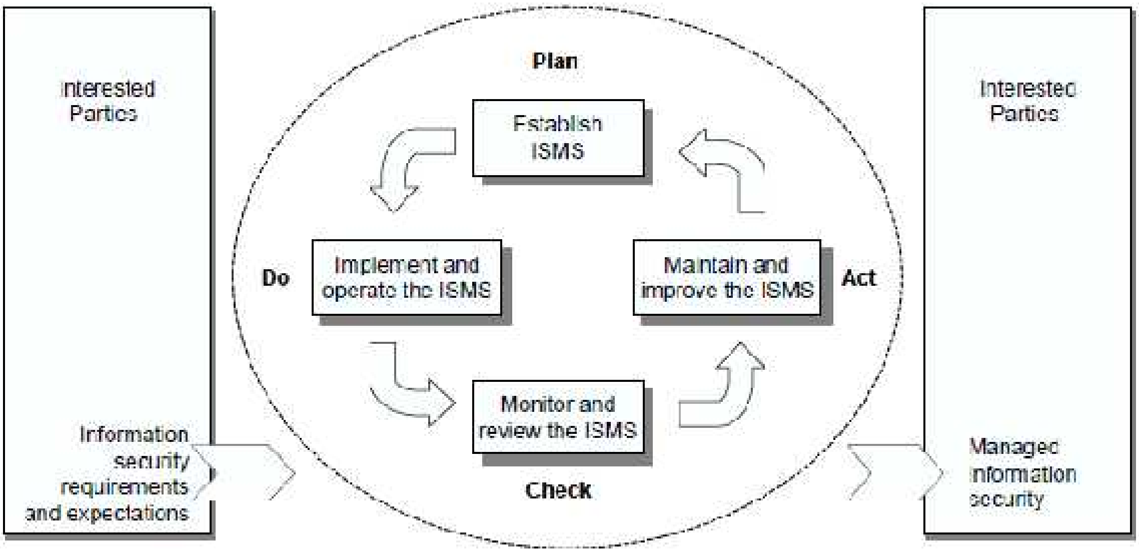


Figure III.2: *PDCA model applied to ISMS processes* [3]

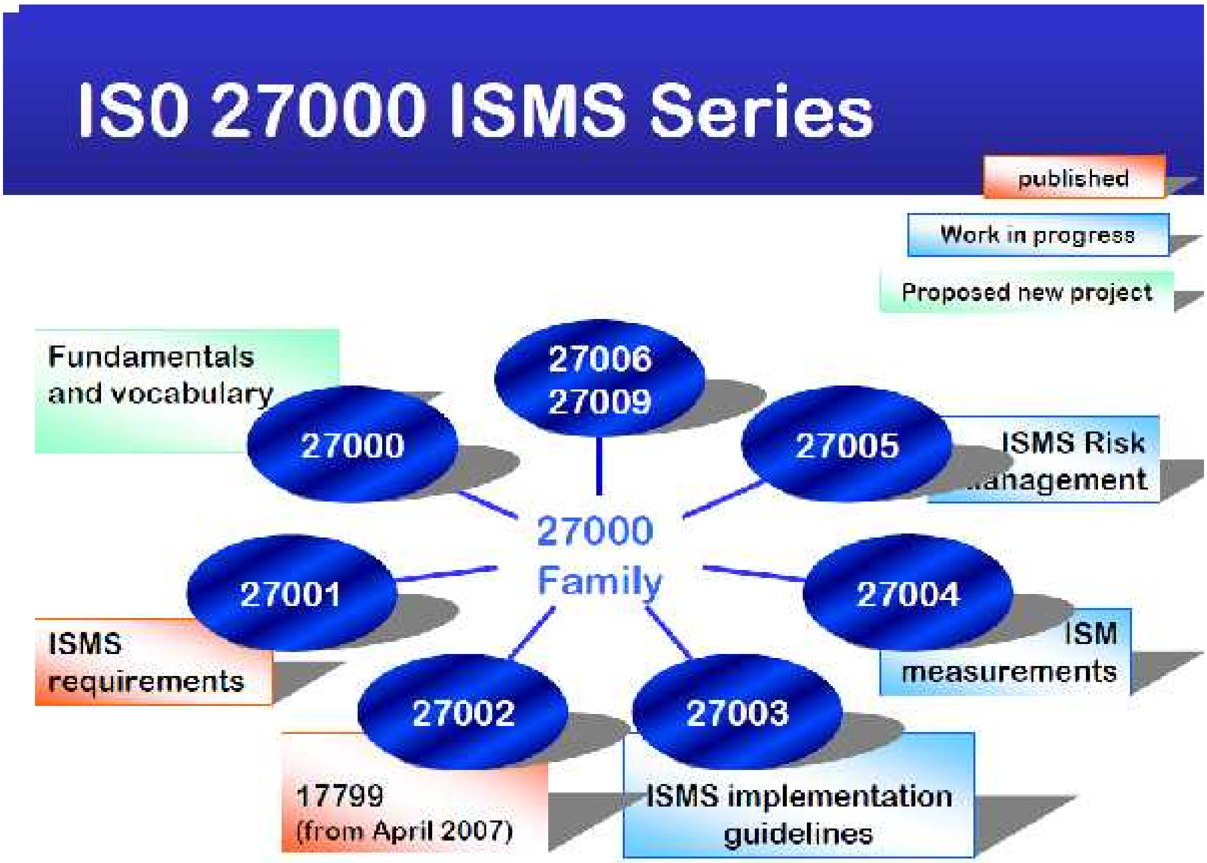
IV. INFORMATION SECURITY STANDARDS

The ISO/IEC 27000-series numbering ("ISO27k") represents a larger family (**Figures V.1, IV.2**) of information security management standards. Developed by a joint committee of the International Standards Organization (ISO) in Geneva and the International Electrotechnical Commission (IEC), these standards now provide a globally recognized framework for good information security management.

The following standards have been published [4]:

- **ISO/IEC 27000:2009** - provides an overview/introduction to the ISO27k standards as a whole plus the specialist vocabulary used in ISO27k.
- **ISO/IEC 27001:2005** is the Information Security Management System (ISMS) requirements standard, a specification for an ISMS against which thousands of organizations have been certified compliant.
- **ISO/IEC 27002:2005** is the code of practice for information security management describing a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.
- **ISO/IEC 27003:2010** provides guidance on implementing ISO/IEC 27001.
- **ISO/IEC 27004:2009** is an information security management measurement standard.
- **ISO/IEC 27005:2011** (2nd edition) is an information security risk management standard.
- **ISO/IEC 27006:2007** is a guide to the certification or registration process for accredited ISMS certification or registration bodies.
- **ISO/IEC 27011:2008** is the information security management guideline for telecommunications organizations (also known as ITU X.1051).
- **ISO/IEC 27031** is an ICT-focused standard on business continuity.
- **ISO/IEC 27033** is replacing the multi-part ISO/IEC 18028 standard on IT network security (part 1 released, rest in preparation).
- **ISO 27799:2008** provides health sector specific ISMS implementation guidance based on ISO/IEC 27002.

IV.1. Tables, symbols, figures, and diagrams:



ISO 27000 ISMS Series

published

Work in progress

Proposed new project

Fundamentals and vocabulary

27000

27006
27009

27005

ISMS Risk management

27000 Family

27001

ISMS requirements

27004

ISM measurements

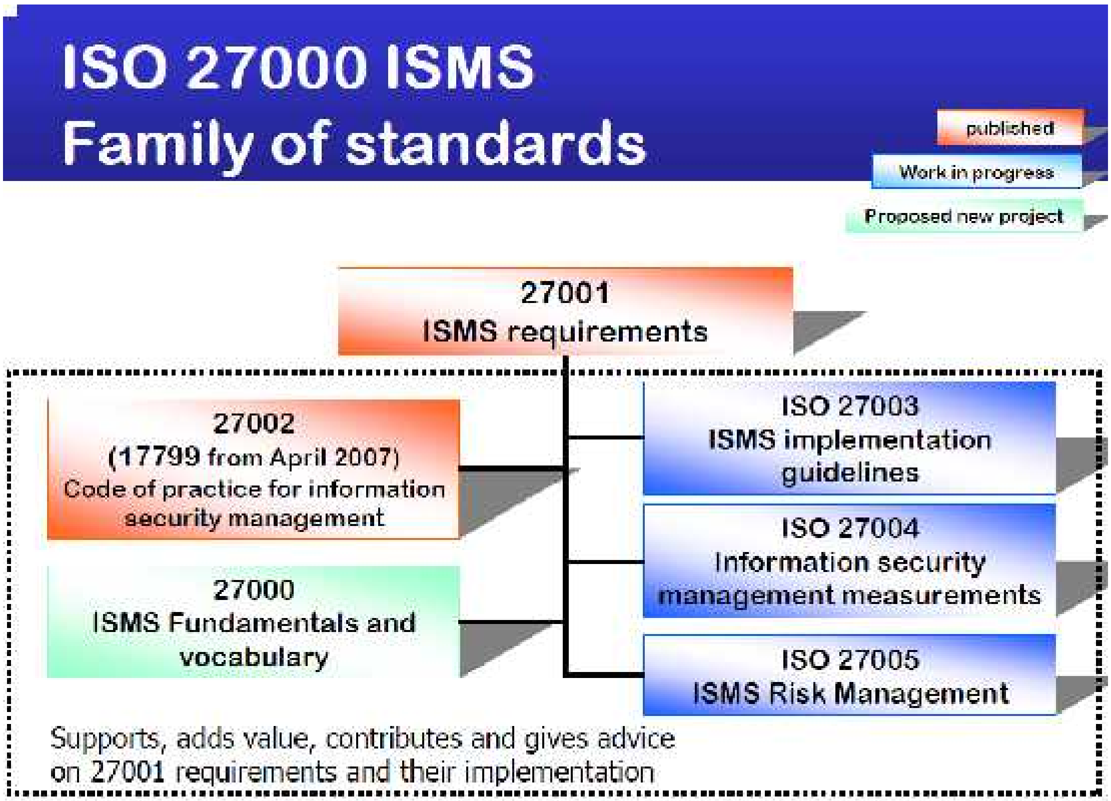
27002

17799 (from April 2007)

27003

ISMS implementation guidelines

Figure IV.1: *ISO/IEC 27000 ISMS International Standard Series*



ISO 27000 ISMS
Family of standards

published

Work in progress

Proposed new project

27001
ISMS requirements

27002
(17799 from April 2007)
Code of practice for information security management

27000
ISMS Fundamentals and vocabulary

ISO 27003
ISMS implementation guidelines

ISO 27004
Information security management measurements

ISO 27005
ISMS Risk Management

Supports, adds value, contributes and gives advice on 27001 requirements and their implementation

Figure IV.2: *ISO/IEC 27001 - Guides of Implementation*

GLOSSARY OF TERMS

asset

anything that has value to the organization

availability

the property of being accessible and usable upon demand by an authorized entity

CEO

Chief Executive Officer

CIO

Chief Information Officer

COBIT

Control Objectives for Information and related Technology

confidentiality

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes

DBA

Database Administrator

ERP

Enterprise resource planning

FICO

Financial Accounting and Controlling

HR

Human Resources

information security

Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

information security event

an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

information security incident

a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

information security management system (ISMS)

that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

integrity

the property of safeguarding the accuracy and completeness of assets

ISM

Information Security Management

ISP

Information Security Policy

IT

Information technology

MM

Material Management

PP

Production Planning

QM

Quality Management

residual risk

the risk remaining after risk treatment

risk acceptance

decision to accept a risk

risk analysis

systematic use of information to identify sources and to estimate the risk

risk assessment

overall process of risk analysis and risk evaluation

risk evaluation

process of comparing the estimated risk against given risk criteria to determine the significance of the risk

risk management

coordinated activities to direct and control an organization with regard to risk

risk treatment

process of selection and implementation of measures to modify risk

SAP

System Analysis and Program Development

SD

Sales and Distribution

statement of applicability

documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS.

CONCLUSION

To the organization, information is one of the most vital asset. In order to protect information, the organization should have proper information security framework in place.

The organization should also make a note that the information security framework is an ongoing process. Continuous improvements, whether in response to environmental incidences or interview reviews, are important to ensure the adequate protection of information resources (Ezingeard & Bowen-Schrire, 2007). To assess the adequacy of current practices, measuring and reporting of risks, control issues, and vulnerabilities are necessary (Purtell, 2007).

In this era of increased cyber attacks and information security breaches, it is essential that all organizations give information security the focus it requires.

To ensure information security, the organization should understand that information security is not solely a technological issue. The organization should also consider the non-technical aspect of information security while developing the information security framework.

REFERENCES

[1] http://people.dsv.su.se/~bjorck/files/thesis-book.pdf

[2] https://www.mercy.edu/ias/patil.pdf

[3] international standard ISO/IEC 27001:2005

[4] http://www.iso27001security.com/html/iso27000.html

[5] http://sst.nsu.edu/ia/education/lectures/csc635/ppts/Ch05.pdf

[6] http://security.calpoly.edu/index.html - *e.g. ISMS -> web page*

[7] http://www.2dix.com/document-pdf/page-1-information-security-in-organizations-pdf.php

[8] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-best_practices_for_managing_information_security-february_2010_OR_2876547.en-us.pdf

[9] http://nitc.ne.gov/standards/security/user_template.pdf

[10] http://nitc.nebraska.gov/tp/meetings/documents/011023/Security_Officers_Guide_print.pdf

[11] http://www.issa.org/Downloads/Whitepapers/Biggest-Information-Security-Mistakes_Security-Innovation.pdf

[12] http://www.is2me.org/IS2ME-EN-V1.0.pdf

HUMAN TRAINING OR TEHNOLOGICAL BOUNDARIES?

CAPT Sorin-Alexandru CATANĂ

INTRODUCTION

Every citizen has the right to engage in community decision-making processes, but also should recognize that its legitimate interests involve promotion and protection of classified information. Information is a product which, like other important products of human activity, is valuable for an organization and therefore must be properly protected. Protective methods of information are varied today, depending on the type of vulnerabilities that it protects. As the theme of this paper says, the protection of information is realized by people and technological tools. In an organization, information security is the responsibility of management at the highest level. The members are only required to follow the rules imposed by management policies and procedures. The policies and procedure have to be developed by management with the support of security and IT departments and they should include also training of the members.

Accelerating changes and the inevitability of future shock, the impact of technology against natural or social environment, the transition from forced technology to high technology require education and a new technological mentality. Information explosion and accelerated depreciation of scientific and technical knowledge, as well as proliferation, diversification and continuous improvement of education technology products require technological education through which man to be better able to master and exploit new technology more efficiently. The cause for which it is difficult to observe the effects of technology on us is that it is part of our existential environment, it became somehow natural in the sense that surrounds us and we can not live without it. *It is our environment*, McLuhan says, *and like any environment (we could make a comparison with the air that surrounds us and not always aware of his presence) is hidden from us, and we have intentionally turn our attention to, to see how it affects us.*[53]

The rows ahead will attempt to answer at the question from the topic, to decide which of these two factors has a higher importance securing information, which are the connections and interdependences between them and also to determine whether there is any situation when the information assurance can be provided from only one of the factors. Is it enough to have a highly skilled human resource, well-motivated, aware of risks involved by insufficient protection of sensitive organization information without a special advised configuration of the working tools?

[53] Pop Ionut Marcel *Fenomenul Internet. O abordare religios-morală*, http://www.nistea.com/media/internet/pop_internet/omul_internetul.htm, 06.09.2011 21.00

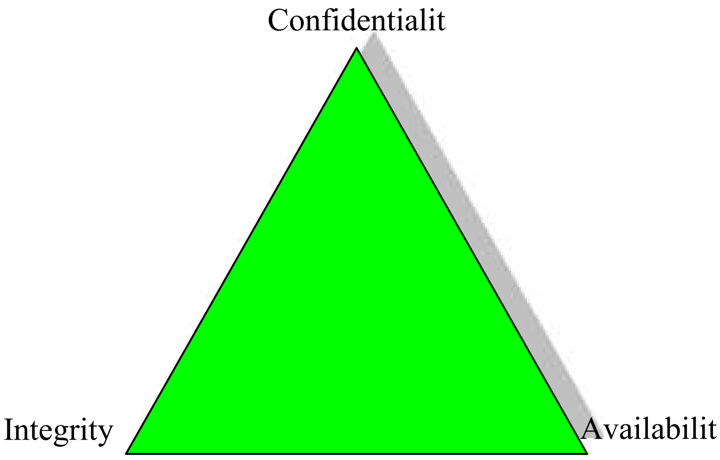
Otherwise, is it sufficient to create a security policy based only on the protection offered by the tools and working environment configuration without awareness of the organization members?

I. INFORMATION ASSURANCE

I.1. Principles of effective information security

Assurance of information is often divided into different classes: human introduced errors, user abuse of authority, power and policy, system probing or mapping, system probing with malicious hardware and software; system penetration, subversion of environment security and control mechanisms.

Information security is a far reaching and often all encompassing topic, but at it's core information security and the protection of digital assets can be reduced to three central attributes. These are Confidentiality, Integrity and Availability; often referred to as the CIA triangle. Each factor provides a different and complementary protection to data and all three must be sufficiently preserved to maintain the useful of the information and information systems that are being protected.[54]



(1) CIA Triad: Confidentiality, Integrity and Availability

- **Confidentiality -** Maintaining data's confidentiality requires ensuring that only those users and/or systems authorized to access the stored information are able to access the protected data.
- **Integrity -** Maintaining data integrity involves ensuring that the data remains correct, whilst in storage or transit, and that only authorized changes are made to the data.
- **Availability -** For any information system to serve its purpose, the information must be available when it is needed. Maintaining availability of both systems and

[54] Information security http://en.wikipedia.org/wiki/Information_security 06.06.2011 13.00

information is crucial for most IT professionals to continue in gainful employment. As a result a lot of tasks geared towards ensuring systems availability are already incorporated into most business practices, including frequent backups and maintaining standby systems to replace production units in the event of a failure.[55]

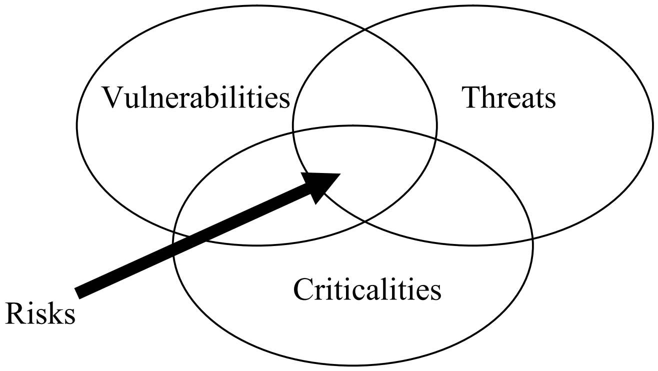
I.2. Risk management in an organization

Both in the organization and in the environment in which it acts, there is uncertainty about the nature of threats in achieving the objectives or about the nature of opportunities. Any manager has to take account of managing the threats, because otherwise, unfulfilling his objectives, he would be disqualified, or to take advantage of opportunities for the benefit of the organization, proving its effectiveness. If uncertainty is a fact of life, then the response to uncertainty should be a constant concern.

Managers of an organization need not to confine themselves to handle, each time, the consequences of events that occurred. Treating the consequences doesn't dress the causes, therefore, the risks have already materialized will occur in the future, usually with a higher frequency and an increased impact on the objectives. Managers should adopt a reactive management style, which means that it is necessary to design and apply measures likely to mitigate the risk event. Future-oriented response allows the organization to master, within reason, past hazards, which is the same with increasing the opportunities to achieve their goals.

Information assurance mechanisms may be subdivided into three categories: preventive, corrective and detective. For all complex systems, there are myriad combinations of protection, detection, and correction mechanisms that will provide similar qualitative levels of information assurance. Risk management is the process of the identification, measurement, control and minimization of security risks in information systems to a level commensurate with the value of the assets protected. The analysis of criticality, vulnerability and threat are the underlying foundations for operational risk evaluation and identification. Risk is greatest where the vulnerability, threat and organization criticality intersect.

[55] Andrew Waite *InfoSec Triads: C.I.A.*, http://blog.infosanity.co.uk/2010/06/07/infosec-triads-c-i-a 06.06.2011 14.00



(2) Risk identification model

Risk identification and management are the function of three variables: criticality, vulnerability and threat. These areas are illustrated in figure two. The first element is criticality – how important is this asset to the organization? The second element is vulnerability – in what ways can the asset be compromised, exploited, damaged or destroyed? The third element is threat – who or what can exploit a vulnerability and what capabilities does that threat have that might be exploited?[56]

I.3. The costs of securing information

Despite prevention efforts, information security breaches are common. The largest body of research related to preventing breaches is technical, focusing on such concerns as encryption and access controls. In contrast, the research related to the economic aspects of information security is small but rapidly growing. Yet, little is known about the budgeting process used in deciding how much to spend on information security.

The costs associated with information security activities relate to a host of items, including hardware, software, and personnel. Most of these expenditures are best thought of as capital investments, although firms tend to treat such costs as operating expenses within the period incurred. Whether they are treated as capital or operating expenditures, budgeting for information security expenditures is a crucial resource allocation decision. From an economics perspective, firms should invest up to the point where the last dollar of information security investment yields a dollar of savings. That is, information security expenditures should be viewed in cost-benefit terms.

Information security should be viewed in the future. If in an organization have not been major incidents and violations of information that does not mean that in the future is no longer necessary allocation of funds for information security. Generally less expensive equipment,

[56] Tim Bass and Roger Robichaux *Defense-In-Depth Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations* - MILCOM 2003

inadequate training of organization members related to information protection and the poor quality and skills of security branch involves a low level of information security.

Threats and vulnerabilities are in a continuous dynamic and they are increasing once with technological development and skills of those who want unauthorized access to sensitive information of the organization for various purposes. Information security should be in the same dynamic to keep up with the new threats and to accomplish this requirement; financial efforts should made by organization.

II. THE IMPORTANCE OF TRAINING FOR INFORMATION ASSURANCE

Almost invariably, security awareness and training are the most cost effective measures that can be employed to protect corporate and organizational information assets. This is largely due to the fact that protecting information, generally more so than other asset, is best achieved through routine practices that permeate every element of an organization. Therefore, where each individual entrusted with sensitive information takes prudent measures and personal responsibility for protecting those assets, a robust security environment should occur naturally.

II.1. Information security awareness

The term “information security awareness” is used to refer to a state where users in an organization are aware of their security mission. Information systems can be useful only if people use them. Similarly, information security awareness is of crucial importance, as information security techniques or procedures can be misused, misinterpreted or not used by end-users, thereby losing their real usefulness.

Increased awareness should minimize ``user related faults", nullify them in theory, and maximize the efficiency of security techniques and procedures from the user point of view.

Although educational or awareness issues (from simply information security guidelines to well-developed information security education programmes) are security matters in nearly all organizations in the era of the information society.

It is generally agreed that performance depends on ability, motivation and working conditions. These factors interact constantly: the effects of motivation on performance depend on ability and vice versa.

The purpose of security awareness, training, and education is to enhance security by:

- improving awareness of the need to protect system resources and information;
- developing skills and knowledge (so computer users can perform their jobs more securely); and

- building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

Making organization members aware of their security responsibilities and teaching those correct practices helps people change their behavior. It also supports individual accountability, which is one of the most important ways to improve organization security. Without knowing the necessary security measures (and how to use them), users cannot be truly accountable for their actions.

Specific activities should be undertaken, such as a security awareness programme, to promote security awareness to all individuals who have access to the information and systems of the organization. The objective is to ensure all relevant individuals understand the key elements of information security and why it is needed, and understand their personal information security responsibilities.

II.2. Staff skills

Staff should be educated/trained in how to run systems correctly and how to develop and apply security controls. The objective is to provide staff with the skills required to run systems correctly and fulfill their information security responsibilities. Education/training should be given to provide staff with the skills they need to assess security requirements, propose security controls and ensure that security controls function effectively in the environments in which they are applied. Education/training should be carried out to provide:

- Systems development staff with the skills they need to design systems in a disciplined manner and develop security controls
- IT staff with the skills they need to run computer installations and networks correctly and apply security controls
- Business users with the skills they need to use systems correctly and apply security controls
- Information security specialists with the skills they need to understand the business, run security projects, communicate effectively, and perform specialist security activities.[57]

Between them there must be well structured communication due to interdependencies and interconnections of each responsibility.

[57] Mikko T. Siponen *A conceptual foundation for organizational information security awareness* http://wotan.liu.edu/docis/lib/sisl/rclis/dbl/imgcsc, 08.06.2011 18.00.

Information security managers must be well versed in the breadth of the IT career field and other disciplines as well (e.g. physical security, accounting and human resources management). In addition, a security manager must be a passionate advocate and an effective communicator. Interpersonal skills should include the ability to communicate in non-technical terms. He must also be able to coordinate all the departments with responsibilities in information security and to have an overview picture of the security system implemented in the organization.

II.3. Communication Feedback

Information security is not solely the job of a few individuals within an organization. Rather, all organization members should be educated and empowered to protect the sensitive data. The goal of communication about security issues is promoting information security, encouraging all employees to make it a priority, and to enforce organization policies and change member's behavior. The decision about how much to communicate is dependent on organization culture and overall information security goals.

Receivers are not just passive absorbers of messages and trainings; they receive the message and respond to them. Feedback is the response of the audience; it enables the manager to evaluate the effectiveness of your message and training. If the audience doesn't understand the meaning, you can tell by the response and then refine the message and the security training accordingly.

Giving your audience a chance to provide feedback is crucial for maintaining an open communication climate. The manager must create an environment that encourages feedback. For example after explaining their security responsibilities to the organization members, the manager must be sure whether they have understood them or not. Also is essential to know whether the recipient has understood the message in the same terms as intended by the sender and whether he agrees to the specific information security tasks that he must act accordingly. Employees are not always willing to provide feedback especially regarding information security. The organization has to work a lot to get the accurate feedback.

Soliciting employee feedback helps managers collecting good ideas and suggestions, and listening to employee concerns. This information can be used to refine information security policies and practices and improve FAQ relevancy.

Sometimes the employees, in their daily activities, discover new threats and vulnerabilities that the security department have not yet considered because of overlooking or technological and activities changes. So aware of the importance of ensuring information security and creating a good two-way communication, employees may contribute to the development of new information protection mechanisms and information security plan.

The manager must ensure that training provided leads to that feedback through which he can verify the effectiveness of information security methods and procedures applied in the organization.

II.4. Information security planning

Information is an essential business asset that organizations must protect along with other important business assets. Information can exist in many forms — print, notes on paper, films, or data stored electronically. People share information via mail or electronic means, and in conversation. Whatever form information takes, whatever means people use to share it, an organization should always secure information appropriately.

Information security is achieved by implementing an appropriate set of politics, practices, procedures, organizational structures, hardware and software functions. These elements must be implemented to the extent that ensures specific security goals.

It is important that each organization to be able to identify their own security requirements. To do this it must appeal to three main sources:

- risk assessment: identify threats to resources, vulnerability to these threats are evaluated and their probability and potential impact is estimated;
- existing legislation that an organization must comply;
- security analysis: the specific set of principles, objectives and requirements for processing information, that the organization develop to support their activities.

To analyze the risks an organization can identify their own security-related requirements. This process generally involves four main steps:

- resources to be protected;
- identifying risks / threats specific to each resource;
- risk ranking;
- identification of controls by that will be removed or reduced the risks.

Security analysis must include the following steps:

- The selection of viable solutions;
- Establishing security assurance strategy;
  - Subdivision and control of connections;
  - Layers protection;
  - Incident response strategy;
  - Allocation of resources for security.
- Establishing security policies;
- Achieving security mechanisms and procedures:

- System documentation;
- Security Certification - periodic monitoring the correspondence between the system functionality and documentation drawn (internal and external audit);
- Evaluation of the security system through security tests - assessing that the documentation and the functioning of security mechanisms satisfies the security needs imposed by environment;
- Security accreditation - the decision of the competent authority (the owner) to authorize the functioning and therefore the residual risk assuming.[58]

To define its security policy organization has to decide:

- which threats must be eliminated and which can be tolerated;
- which resources should be protected and at what level;
- which measures should be taken to implement the security;
- what is the price (financial, human, social, etc..) of the security measures that can be accepted.

III. INFORMATION SECURITY THROUGH TECHNOLOGY

Security is a basic human concept that has become more difficult to define and enforce in the Information Age. In primitive societies, security was limited to ensuring the safety of the group's members and protecting physical resources, like food and water. As society has grown more complex, the significance of sharing and securing the important resource of information has increased. Before the proliferation of modern communications, information security was limited to controlling physical access to oral or written communications. The importance of information security led societies to develop innovative ways of protecting their information. For example, the Roman Empire's military wrote sensitive messages on parchments that could be dissolved in water after they had been read. Military history provides another more recent example of the importance of information security. Decades after World War II ended, it was revealed that the Allies had gained an enormous advantage by deciphering both the German and Japanese encryption codes early in the conflict. Recent innovations in information technology, like the Internet, have made it possible to send vast quantities of data across the globe with ease. However, the challenge of controlling and protecting that information has grown exponentially now that data can be easily transmitted, stored, copied, manipulated, and destroyed.

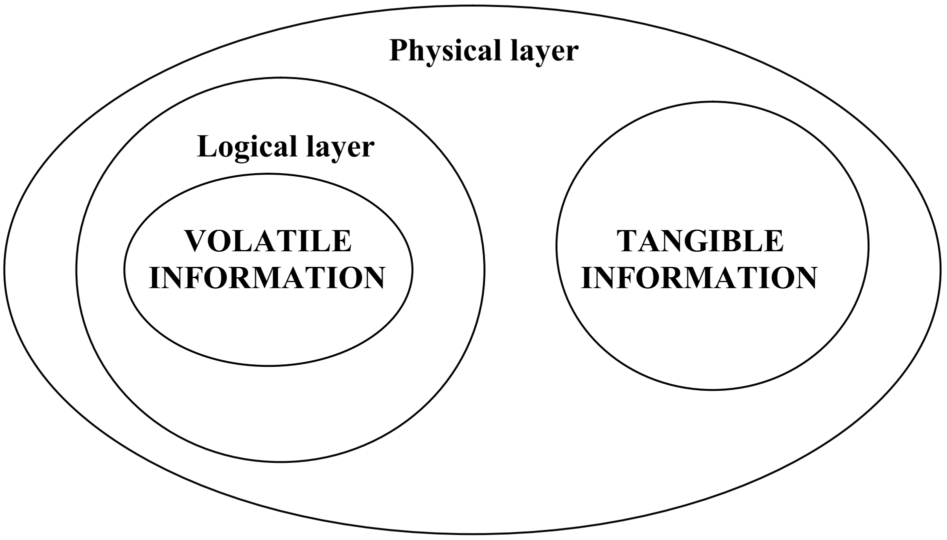
[58] *Asigurarea securitatii informatiilor* http://www.securitatea-informatiilor.ro/audit-de-securitate/asigurarea-securitatii-informatiilor-129.html 08.06.2011 20.00

Within large organization information technology generally refers to laptop and desktop computers, servers, routers, and switches that form a computer network, although information technology also includes fax machines, phone and voice mail systems, cellular phones, and other electronic systems. A growing reliance on computers to work and communicate has made the control of computer networks an important part of information security. Unauthorized access to paper documents or phone conversations is still an information security concern, but the real challenge has become protecting the security of computer networks, especially when they are connected to the Internet. Most large organizations have their own local computer network, or intranet, that links their computers together to share resources and support the communications of employees and others with a legitimate need for access. Some of these networks are connected to the Internet and allow employees to go "online."

Computer hacks aren't just about bits and bytes; they can have real, quantifiable and destructive outcomes. Nobody would contest that organizations require physical security; further, very few organizations would even consider doing business without some type of IT security. Prudence dictates that for physical threats, physical monitoring solutions be leveraged to mitigate risk. If there are logical threats, then logical monitoring solutions should be used. And, if the threats converge, then the security solutions must converge as well. This sounds simple, but the disciplines of physical and logical security are highly disparate. As such, getting the technology and the individuals to work synergistically can be challenging.[59]

We can talk about two different layers of protection, one physical and one logical and two types of information states a tangible (physical) one, and a volatile (logical) one. According to this model fig.3, to gain access to electronic information is required passing through both layers and to physical information only through physical layer.

[59] Brian T. Contos, *The Convergence of Logical and Physical Security Solutions*, IT DEFENSE august 2006



(3) Security layers model

Physical and logical security staffs have the same goal -protect enterprise assets- yet they exist as independent factions, and not always peacefully. To truly gain a global perspective of an organization's security posture and provide the right level of incident detection, physical and logical security solutions must converge.

III.1. Physical security

Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

Physical security describes measures that are designed to deny access to unauthorized personnel (including attackers) from physically accessing a building, facility, resource, or stored information; and guidance on how to design structures to resist potentially hostile acts. The technology used for physical security has changed over time. While in past eras, there was no passive infrared (PIR) based technology, electronic access control systems, or video surveillance system (VSS) cameras, the essential methodology of physical security has not altered over time. Physical security can be as simple as a locked door or as elaborate as multiple layers of barriers, armed security guards and guardhouse placement.

Good physical security uses the concept of layered defense, in appropriate combinations to deter and delay intrusions (passive defense), and detect and respond to intrusions (active defense). Ultimately it should be too difficult, risky or costly to an attacker to even attempt an intrusion. However, strong security measures also come at a cost, and there can be no perfect security. It is up to a security designer to balance security features and a tolerable amount of personnel access against available resources, risks to assets to be protected and even aesthetics. There are also life-cycle sustaining costs to consider.

Fundamentally, good physical security is a combination of defensive principles designed to:

- deter
- delay
- detect, and
- respond (and ultimately, deny access)

... to intrusions into critical physical spaces. The first two actions of deter and delay are considered passive defense, while the remaining are active in nature.[60]

However, breaches of physical security can be carried out with little or no technical knowledge on the part of an attacker. Moreover, accidents and natural disasters are a part of everyday life, and in the long term, are inevitable.

There are three main components to physical security. First, obstacles can be placed in the way of potential attackers and sites can be hardened against accidents and environmental disasters. Such measures can include multiple locks, fencing, walls, fireproof safes, and water sprinklers. Second, surveillance and notification systems can be put in place, such as lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras. Third, methods can be implemented to apprehend attackers (preferably before any damage has been done) and to recover quickly from accidents, fires, or natural disasters.

III.2. Logical security

Logical Security consists of software safeguards for an organization's systems, including user identification and password access, authentication, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation. It is a subset of computer security.

Logical security should start at the lowest level, the OS, and moves up with securing the desktop functions and usability of applications. When we talk about logical security, we must establish what specific elements should be protected and by what methods.

Issues that must be protected:

- Storage of data
- Data access
- Communication

Some of the logical methods to ensure the safety of data **storage** are creating backups and using the redundancy systems. Backups are used to not having the information stored on one single

[60] *Physical security* http://en.wikipedia.org/wiki/Physical_security 10.06.2011 18.00

memory medium in one single place. Can be done automatically by computer systems or manually at the established times and periods. Redundancy systems are designed to replace the systems in operation. They must provide identical services to the users and to the other systems interconnected with, as the base system.

Security of access is assured by authentication, access rights and authority levels, firewalls, intrusion detection systems. All these elements are intended to leave no unauthorized access to sensitive information of the organization. Authentication is the process used by a computer program, computer, or network to attempt to confirm the identity of a user. It can be done through several methods:

- user ID and password;
- biometrics authentication;
- token-authentication.

User ID and password authentication uses secret data to control access to a particular resource. Usually, the user attempting to access the network, computer or computer program is queried on whether they know the password or not, and is granted or denied access accordingly.

Biometrics authentication is the measuring of a user's physiological or behavioral features to attempt to confirm his/her identity.

Token Authentication comprises security tokens which are small devices that authorized users of computer systems or networks carry to assist in identifying that who is logging in to a computer or network system is actually authorized.

Firewalls are technological barriers designed to prevent unauthorized or unwanted access and communication to a computers network or host.

An intrusion detection system (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a management station. It can be change into a intrusion prevention system (IPS) which can stop the traffic before something harmful happens.

Security of **communication** is assured by antivirus programs, software, firewalls, IDS, encryption of data, public key infrastructure and using of virtual private networks.

III.3. What the future reserves us?

Information technology security is often the challenge of balancing the demands of users versus the need for data confidentiality, integrity and availability. For example, allowing employees to access a network from a remote location, like their home or a project site, can increase the value of the network and efficiency of the employee. Unfortunately, remote access to a network also opens a number of vulnerabilities and creates difficult security challenges for a network administrator.[61]

Solutions offered by antivirus, antispam, antispyware, firewall equipment or programs, VPN programs, intrusion detection and prevention (IDS, IPS) or information encryption methods are widely used by all those who are aware of communication risks in the internet age.

It's obvious why people sometimes fail to use IT security features correctly: IT is difficult for nontechnical people to understand. What's more, even technical people struggle with complex modern technologies and nobody is an expert in all fields.

Computers cannot be made consistently more powerful and remain safe if they are not endowed with the power not only to input and output bytes but understand them. But, having taught them to listen and speak we must simultaneously teach them proper manners. As computers become smarter, more sophisticated, and more flexible, they will become more like us. That is, they will acquire the reliable information security provisions that all of us carry around as our basic make-up. Yet, as they become more like us, they will begin to ingest information at the semantic level from outside sources as we do, and will thus be heir to more subtle but no less problematic forms of information warfare. Or, to put it simply: today's problems will pass and tomorrow's will rise.[62]

Overall, near-term prospects favor greater information security. True, closed systems are continuing to open up and the number of opportunities for waging computer warfare continues to rise. Yet, protection tools are becoming better, the Internet is likely to become more secure, the costs of backup and redundancy are likely to fall sharply, and cryptographic methods are likely to spread.

CONCLUSIONS

Information is the lifeblood of organizations, a vital business asset in today's IT-enabled world.

IT systems and networks link every internal department and connect us with a immensity of suppliers, partners and markets. Access to high-quality, complete, accurate and up-to-date information makes managerial decision-making relatively easy by reducing the margin for error.

Man is not only the pillar and the creator of technology, but is also a reverse process by which people become addicted to technology and they are formed by it. But although the technique shows rigidity, it opens a vast field of alternatives and may be subject to very different applications. Each of us for whom the computer has become a common object but necessary, we woke up at least once on the verge of anger, wanting desperately to make computer dust. And

[61] *Network security resources* http://www.ischool.utexas.edu/~netsec/overview.html, 08.06.2011 20.00

[62] Martin Libicki *The Future of Information Security* http://www.fas.org/irp/threat/cyber/docs/infosec.htm 10.06.2011 16.30

some have even succeeded. Then, desperate because they had lost important information, resorted to everything they knew from anywhere, from sources more or less authorized to repair the damage done. (For that, we must admit, the man is enemy no. one of the computers!). The direction of evolution depends of human: to progress, order and perfection or to self-destruct - which must impose a high morality and accountability in the use of massive energy and high technologies that today man can have. So, in conclusion, man is turning to technology to make his life easier, but also, he needs a higher intelligence at an early age so that it can maintain the technological balance.63

As developers invent new and better security technologies, making increasingly difficult exploitation of technological vulnerabilities, hackers will turn increasingly to the exploitation of human element. Breaking the human protective wall can often be easily, without requiring any investment other than the cost of a phone call and involving minimal risk.

Effective security awareness programs need to find a balance between glossing -over important points and getting buried in the jargon, acronyms and fine details all too common in technical manuals. It is vital that awareness materials are written in a clear yet engaging style and that the information content is interesting, relevant and useful. This is arguably the biggest challenge in security awareness.

Security guru Bruce Schneier said "*Computers and networks might be difficult to secure, but the biggest security vulnerability is still that link between keyboard and chair. People are sloppy with security; they choose lousy passwords, don't properly delete critical files, and they bypass security policies. They're susceptible to social engineering, and they fall victim to phishing attacks. They misconfigure security hardware and software. They accidentally bring worms and Trojan horses into the network. In short, they're a huge security problem. ... Most of the time security problems are inherently people problems, and technologies don't help much. Photo IDs are a great example. Technologists want to add this and that technology to make IDs harder to forge, but I worry about people bribing issuing officials and getting real IDs in fake names. Technology that makes the IDs harder to forge doesn't solve that problem.*" Bruce describes what he calls **semantic attacks** (some refer to cognitive hacking) that target the human users rather than the computers themselves. He is also reported to have said "*Always remember: amateurs hack systems. Professionals hack people.*"[64]

[63] *Omul si tehnologia* http://ro.shvoong.com/internet-and-technologies/computers/498495-omul-si-tehnologia/ 09.06.201113.00

[64] Dr Gary Hinson The true value of information security awareness

http://www.noticebored.com/html/why_awareness_.html 12.06.2011 18.00

As we have seen throughout this paper, we can not talk about information security only in one of the terms technological or human. If in times long gone information security depended mainly by human factors (motivation, training and awareness), technological development over the past century has increased the share of the technological factor in ensuring information security. Depending on the type of organization (profile, goals) and its available resources, information security chief must find the right balance between technical security measures implemented and security training.

Let's not forget that technological tools have been designed by humans to ease their work and serve their interests. So we must see the technology (exactly what it is) a tool in the hands of man, but a tool that works primarily to reshape the man.

REFERENCES

[1] Pop Ionut Marcel - *Fenomenul Internet. O abordare religios-morală*, http://www.nistea.com/media/internet/pop_internet/omul_internetul.htm, 06.09.2011 21.00;

[2] Information security - http://en.wikipedia.org/wiki/Information_security, 06.06.2011 13.00

[3] Andrew Waite - *InfoSec Triads: C.I.A.*, http://blog.infosanity.co.uk/2010/06/07/infosec-triads-c-i-a, 06.06.2011 14.00

[4] Tim Bass and Roger Robichaux - *Defense-In-Depth Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations* - MILCOM 2003

[5] Mikko T. Siponen - *A conceptual foundation for organizational information security awareness* http://wotan.liu.edu/docis/lib/sisl/rclis/dbl/imgcsc, 08.06.2011 18.00

[6] *Asigurarea securitatii informatiilor* http://www.securitatea-informatiilor.ro/audit-de-securitate/asigurarea-securitatii-informatiilor-129.html, 08.06.2011 20.00

[7] Brian T. Contos - *The Convergence of Logical and Physical Security Solutions*, IT DEFENSE august 2006

[8] *Physical security* http://en.wikipedia.org/wiki/Physical_security 10.06.2011 18.00

[9] *Network security resources* http://www.ischool.utexas.edu/~netsec/overview.html, 08.06.2011 20.00

[10] Martin Libicki - *The Future of Information Security* http://www.fas.org/irp/threat/cyber/docs/infosec.html, 10.06.2011 16.30

[11] *Omul si tehnologia* http://ro.shvoong.com/internet-and-technologies/computers/498495-omul-si-tehnologia/, 09.06.201113.00

[12] Dr Gary Hinson - *The true value of information security awareness* http://www.noticebored.com/html/why_awareness_.html, 12.06.2011 18.00

IDENTITY MANAGEMENT

CPT Srećko JOVANOVIĆ

INTRODUCTION

Identity is defined as the quality or condition of being the same; absolute or essential sameness; oneness. Identity is what makes something or someone the same today as it, she, or he was yesterday. Identity can refer to a thing or a person. Things and people can have different identities when working with different systems, or can have more than one identity when working with a single system.

In nowadays, global and electronic world, identity became a very important issue. Identity management should provide solution for reliable identity verification in time of globalization of business and the increasing integration of information technology.

In close relations with identity is authentication. Authentication is the process of gaining confidence in a claimed identity. Authentication can be based on something which person has (token, card), something he knows (password, PIN) and something he is (physiological characteristic like finger print, facial image).

Smart cards technology with public key infrastructure and biometry provide the best solution for reliable and efficient identity management and strong authentication. In this paper focus will be on Public key infrastructure, smart cards technology and electronic identification documents.

I. Public key infrastructure

Public key infrastructure (PKI) is based on public key cryptography and asymmetric encryption. It provides all security mechanisms: authentication, integrity, non-repudiation and confidentiality. Public key infrastructure provides scalable and open solutions for all system which requiring strong authentication and identity verification. Basics of asymmetric encryption, digital certificates and PKI are explained in this chapter.

I.1. Asymmetric cryptography

Symmetric cryptography has been used for at least 4000 years. On the other hand, asymmetric cryptography is quite new and it was publicly introduced by Whitfield Diffie, Martin Hellman and Ralph Merkle in 1976. Asymmetric algorithms are very different from symmetric algorithms: symmetric algorithms use the same secret key for encryption and decryption, whereas asymmetric algorithms use different keys for encryption and decryption; asymmetric algorithms use more complex mathematical calculation and much longer keys.

Symmetric crypto system is shown in the figure 1. In order to establish secure communication both side (Alice as sender and Bob as recipient) have to have same encryption algorithm and same shared key. Alice calculates cipher text based on secret key and encryption algorithm. Cipher text can be sent over insecure channel because it is unreadable for anyone who does not have secret key. After receiving cipher text, Bob calculates plain text based on same secret key and encryption algorithm. Symmetric encryption has a few problems. First is key distribution: the key must be established between communication participants using secure channel. If we somehow solve key distribution problem, there are also problem with number of keys. If each pair of users needs a separate pair of keys in a network with n users, there are n*(n-1)/2 key pairs, and every user has to store n−1 keys securely. Even for the mid-size networks, company with 2000 people, this requires about 2 million key pairs that must be generated and transported via secure channels. The most important issue with symmetric encryption is that it provides only confidentiality without other security mechanisms: authentication, integrity and non-repudiation.

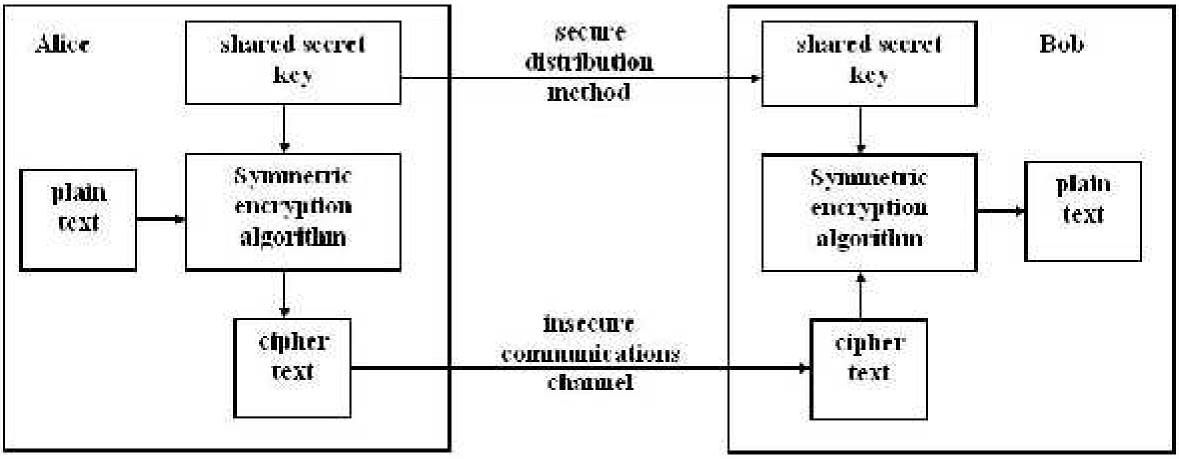
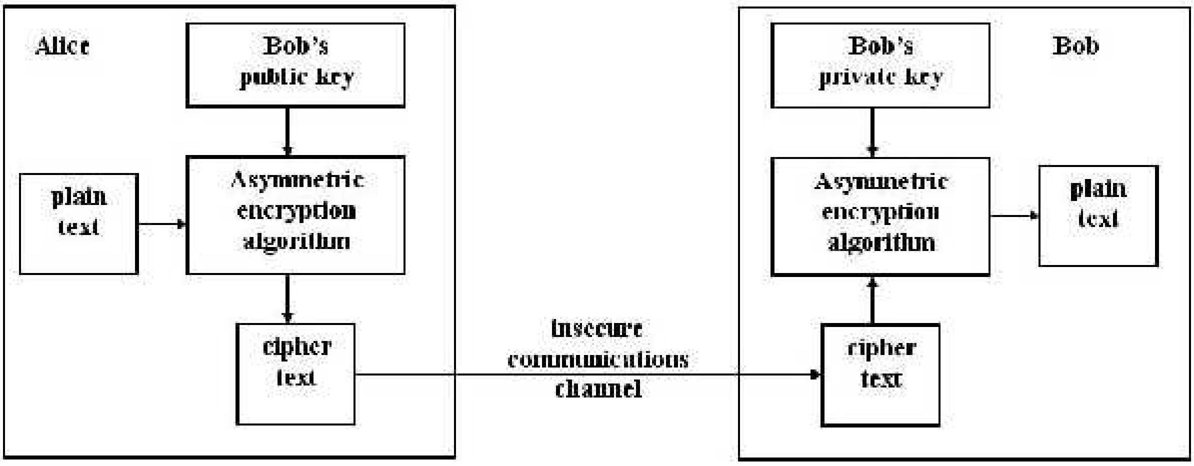

Alice
shared secret key
plain text
Symmetric encryption algorithm
cipher text
secure distribution method
insecure communications channel
Bob
shared secret key
Symmetric encryption algorithm
plain text
cipher text

Figure 1

Asymmetric encryption provides all security mechanisms: confidentiality, integrity, authentication, and non-repudiation. Asymmetric encryption is based on algorithms which use different key for encryption and decryption. One of them is public and one is private or secret. If plain text is encrypted with public key it is possible to decrypt it only with private key and vice versa. In this way, we do not need prior exchange of keys and key distribution. Every participant in communication has pair of keys, private and public. Private key is secret and public key is known by everyone. Basic protocol of public-key encryption is shown in the figure 2.

There are two parts in communication, Alice as a sender, and Bob as a recipient. Alice has Bob's public key because it is published, but only Bob has his private key. Alice encrypts plain text with Bob's public key and sends cipher text over insecure channel. Only the Bob's private key can decrypt this message. This is example of using asymmetric encryption in order to provide confidentiality. Digital signature is technique which is used to provide other security mechanisms: authentication, integrity and non-repudiation. In combination with digital envelope it provides also confidentiality.



Alice
Bob's public key
plain text
Asymmetric encryption algorithm
cipher text
insecure communications channel
Bob's private key
Bob
Asymmetric encryption algorithm
plain text
cipher text

Figure 2

The digital signature concept is shown in figure 3. Picture illustrates Alice as a sender using a digital signature to send message to Bob as a receiver. Process of digital signing consists of several steps:

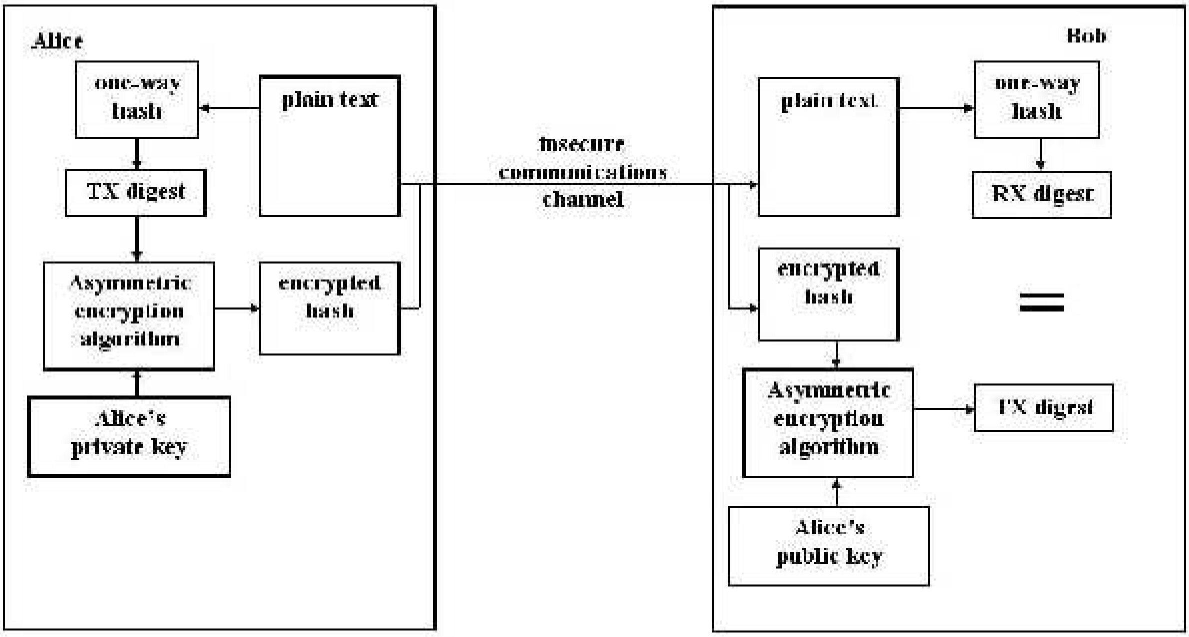


Figure 3

1. Alice calculates message digest or hash. The hash provides a unique value for the message which will later be used by Bob to test the validity and integrity of the message.

2. Alice signs or encrypts hash with his private key. This signing provides message integrity because recipient is assured that only sender could have generated the signature because only he has access to the private key used to sign the hash.
3. Alice concatenates the message and the encrypted hash and sends to Bob original message with encrypted hash.
4. Bob takes the message and the encrypted hash he received from Alice. He decrypts encrypted hash with Alice's public key.
5. Bob calculates hash from the original message and compares it with one which he decrypted. If they match he is assured of the message's integrity and authenticity of the sender.

Digital envelope is technique which is used in order to provide confidentiality using asymmetric encryption. Due to its complexity it is not practical to use asymmetric algorithm to encrypt whole message. Because of that, message is encrypted with symmetric encryption and only symmetric key is encrypted with asymmetric encryption. The process of making digital envelope consists of following steps:

1. Sender encrypts plain text with symmetric key and encrypts symmetric key with recipient's public key.
2. Sender sends to recipient encrypted message and encrypted symmetric key over insecure channel.
3. Recipient takes the encrypted message and encrypted symmetric key. He decrypts symmetric key with his private key.
4. Recipient decrypts cipher text with symmetric key. On this way, message confidentiality is assured because only recipient can access his private key.

The most used asymmetric crypto algorithms are RSA (acronym for Rivest, Shamir and Adleman who first publicly described it), DSA (Digital signature algorithm) and ECDSA (Elliptic curve DSA).

Public keys should be published to provide other users to use them. There is a potential problem: how to be certain whose is a particular public key. This solves the digital certificates which are explained in the next section.

I.2. Digital certificates

Digital certificate is an electronic document which uses a digital signature to bind a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. It connects data about user identity with public keys which are used for encryption and digital signing. Digital certificate is issued and digitally signed by Certification authority - CA. All participants in communication have trust to CA.

The most used certificates format is X.509 which is ITU-T standard for public key cryptography. It is described in RFC 3280. X.509 version 3 provides support for Certificate revocation list (CRL). It contains following attributes:

Version
Serial Number
Signature Algorithm
Issuer
Valid From
Valid To
Subject
Public Key
Extension
Digital Signature

The extensions are specific to the X.509 version 3 certificate. Extensions could be marked as a critical or non-critical. Some extensions must be marked as critical, for other it is recommended to be marked as non-critical. Standard extensions in the certificate are:

Authority Key Identifier
Subject Key Identifier
Key Usage
Private Key Usage Period
Certificate Policies
Policy Mappings
Subject Alternative Name
Issuer Alternative Name
Subject Directory Attributes
Basic Constraints
Name Constraints
Policy Constraints
Extended Key Usage
CRL (Certificate Revocation List) Distribution Points

To summarize, digital certificates represent electronic equivalent to digital ID or digital passport. Public key infrastructure (PKI) systems provide all necessary components for reliable using of digital certificates. Overview of PKI components is given in the next section.

I.3. PKI components

PKI are combination of hardware, software, policy and procedures. PKI system consists of following basic components:

- Basic documents: Certification policy – CP and Certificate practice statement – CPS. Certificate Policy establishes basic principles of certification authority and other components of PKI system. Certificate practice statement is a document that describes practical operation of certification authority.
- Certification authority (CA) is most important component of PKI system which task is management of digital certificates during life cycle. Basic tasks of CA are: issuing of digital certificates, management of certification validity and certificate revocation and publishing Certificate Revocation List – CRL.
- Registration authority (RA) provides interface between users and Certification authority. RA accepts requests, checks user authenticity and forwards standard request for issuing digital certificate.
- System for certificate distribution provides different way for distribution of issued user certificates. Nowadays, smart cards represent the most common method of certificate distribution to users.
- PKI applications are applications which use digital certificates and digital signing technology and may be: protection of web transactions, protection of e-mail service, virtual private networks (VPN), secure electronic document management system, identity and access management systems, etc.

Relations between PKI components are shown in figure 4. Descriptions of specific relations are following:

a) initial registration/certification;

b) renewal of pair of keys, updating of pair of keys, certificate updating, requesting for certificate revocation;

c) certificates publishing and CRL publishing;

d) certificate verification.

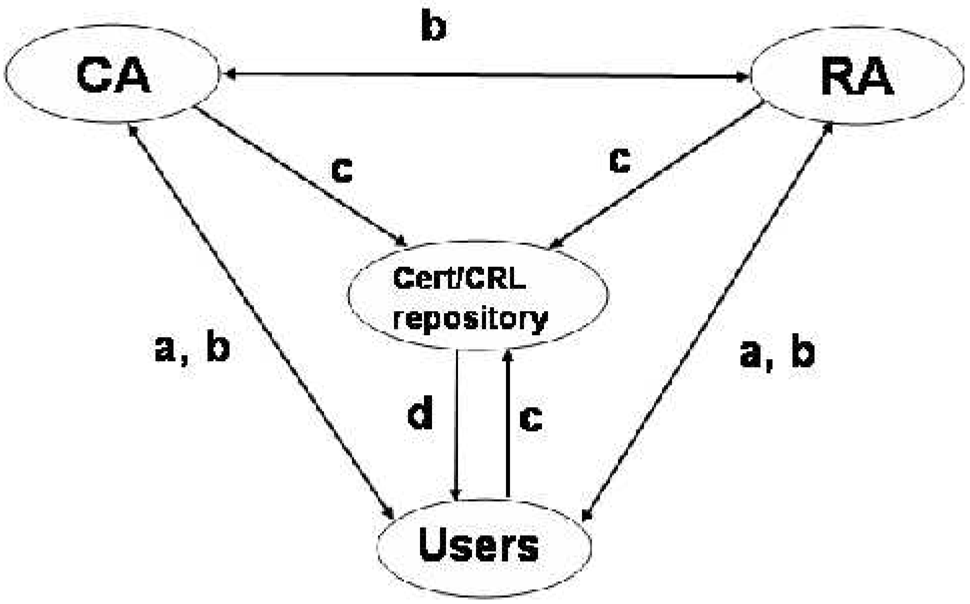


Figure 4

II. Smart cards technology

Smart cards have a very wide field of application. They are, actually, small computers in one square centimeter chip. Because of that, smart cards are appropriate for implementing different application, especially they can be used like a carriers of sensitive data including cryptographic parameters and biometric data. History of using cards, smart card technology and some of smart cards application are described in this chapter.

II.1. History of using cards

Using of plastic cards begins in 1950's in the USA. The first issued plastic card was belonged to the Diners Club. The card was used as a means of payment and to identify the owner. It was used only to store data with basic protection. The card body contained the name of the publisher and embossed owner's name with his signature. Identity protection was based only on visual elements printed on the card and owner's signature. Embossed card was not machine readable. Magnetic cards were appeared as a next improvement. Magnetic card was contained digital record that was readable by a special reader. It was introduced a new way of identifying users through a special number PIN (Personal Identification Number). New technology also had a weakness because with the appropriate equipment it was possible to read, write, alter and delete data. Because of that it was appeared idea to use integrated circuit or microchip on cards for identification. The first use of the card with integrated circuit was in 1984 in France, where the card used in telephony system. A similar project was realized in Germany. The stated card had memory chip, in France EPROM and in Germany EEPROM. The logic of these cards was non programmable and prevented the changing values of the remaining credit on the card. The first cards with microprocessors were used in the German analogue mobile phone network in 1988. After that smart cards are beginning to be used in digital mobile network and later in the financial sector. Today, smart cards have a wide field of use. They are used as credit cards, SIM cards, for access control, and with biometry in identity documents such as ID cards and passports.

II.2. Smart cards

A smart card is a device that includes an embedded integrated circuit chip (ICC) that can be either a secure microcontroller with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signature) and interact intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, subscriber identity modules (SIM) used in GSM mobile phones etc.

Categorization of smart cards is shown on picture 5. According to chip type it may be memory or microprocessor card. According to way of transmitting data smart cards may be contact, contactless and with dual-interface.

Contact smart cards have a contact area about 1 square centimeter. Card must be inserted into a smart card reader with a direct connection to a conductive contact plate on the surface of the card. Standard ISO/IEC 7816 defines electrical connector positions and shapes, electrical characteristic, communication protocols and basic functionality. Smart card communicates with host device through serial interface. Interface description and pinout are shown in figure 6. Card does not have batteries and power is supplied by the card reader.

Contactless smart cards require close proximity to a card reader. The card and the reader have antennae and they communicate using radio frequencies. Contactless smart cards do not have internal power source and derive power from electromagnetic signal. Physical characteristic and transmission protocol for contactless cards are defined in ISO/IEC 14443 standard.

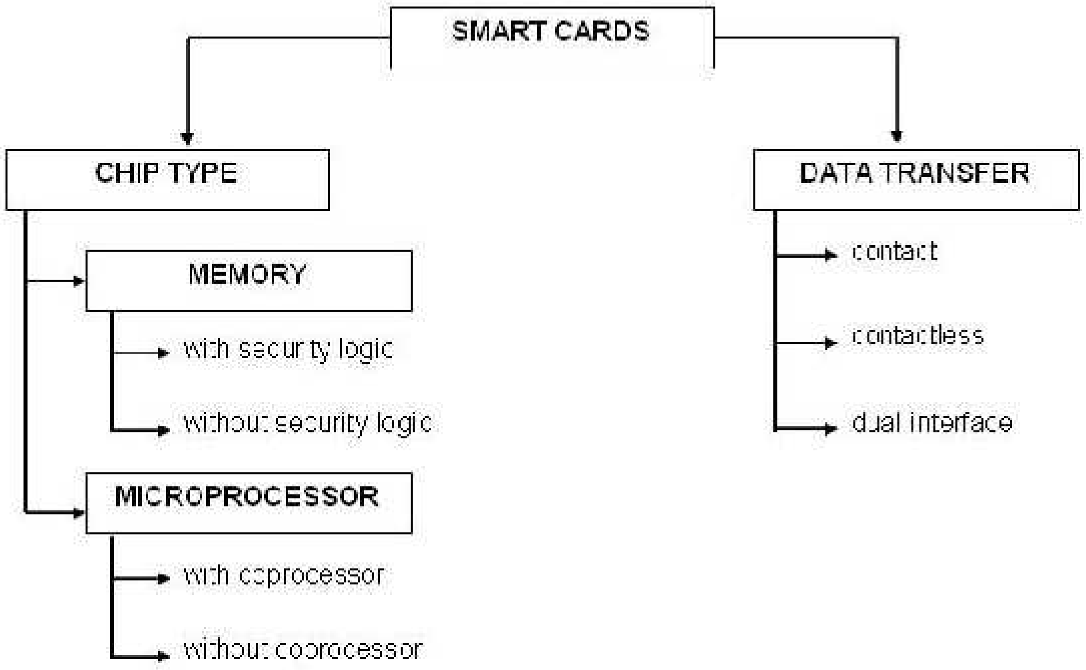
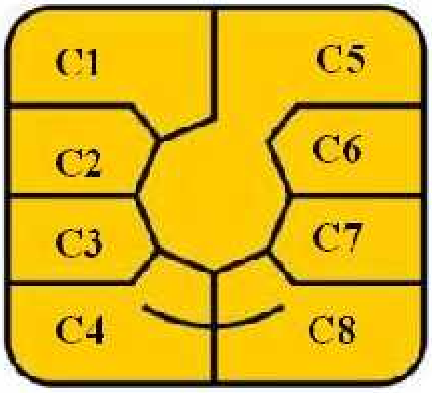
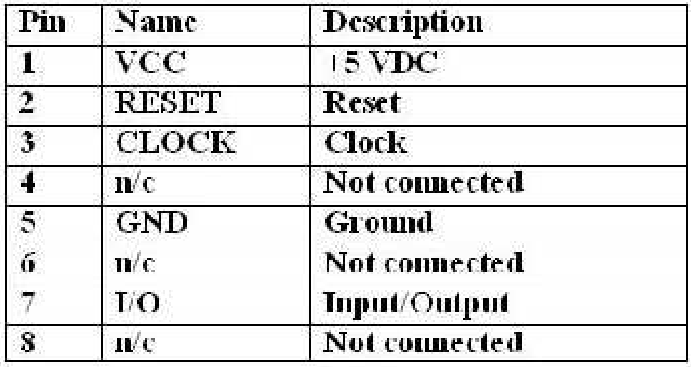


Figure 5





Pin	Name	Description
1	VCC	+5 VDC
2	RESET	Reset
3	CLOCK	Clock
4	n/c	Not connected
5	GND	Ground
6	n/c	Not connected
7	I/O	Input/Output
8	n/c	Not connected

Figure 6

Dual-interface smart cards have both contact and contactless interface on the same chip. There are also hybrid card which has two chips, one with contact interface and one with contactless interface and they are not interconnected.

Memory smart cards have only memory chip (EPROM or EEPROM) and, optionally, could have non programmable secure logic. Microprocessor smart cards have functionality like a personal computer. They have input-output I/O block, ROM memory which is used for storing card operating system (COS), EEPROM memory for storing applications and data, microprocessor and in some cases coprocessor form implementing specific functions. Smart card processor may be 8-bit, 16-bit and 32-bit microcontrollers. Memory of the smart card is protected from unauthorized access. Because of that, storing sensitive data like cryptographic keys, digital certificates, biometric data and passwords are more secure than storing on other media. Card has part of memory which is accessible and other part protected by PIN for storing cryptographic parameters.

Using of smart card depend on operating system implemented on its chip. According to operating system smart cards can be: smart cards with private operating system, MULTOS (Multi-Application Operating System for Smart Cards) cards and Java cards. Smart cards with private operating system are most used cards and their basic characteristics are: low cost, ability to work with 8-bit microprocessors, small capability of customizing implemented card functions and they are usually have one application. MULTOS and Java cards provide better capability for customization. They have implemented virtual machine which executes on card Java applets or MULTOS ALUs (Application Load Unit) defined by user. MULTOS and Java cards permit the loading and deleting of applications at any point in the card's active life cycle.

Smart cards with cryptographic coprocessor are very suitable for using within PKI infrastructure. They provide following functionality:

- generating pair of keys of asymmetric cryptographic algorithm.
- secure storing of cryptographic parameters; keys are stored in protected part of memory and there are no possibility to asymmetric private key be read from card.
- generating digital signature on the card.
- In order to use smart cards within PKI infrastructure it is necessary to have following:
- smart card with chip which has implemented asymmetric crypto algorithm (e.g., RSA coprocessor).
- installed application on smart card which can store several pairs asymmetric private key – certificate.
- smart card reader with appropriate driver installed on host computer or another device.
- middleware software which is provided by card operating system producer. Middleware is interface between card operating system and host application and may be CSP (Cryptographic service provider) for Microsoft application or PKCS#11 libraries for non Microsoft application.

Smart cards support storing biometric data like fingerprint, photo etc. With digital certificate, biometric data and PIN they provide three-factor authentication: based on something that person has (digital certificate), that he knows (PIN number) and that he is (biometric data). Biometric data are stored in card memory and never leave the card. Matching of captured and original biometric are executed within smart card reducing possibility of compromise. Due to their characteristics, smart cards are used in many applications that require highly reliable authentication and identity determination.

II.3. Smart cards applications

Smart cards have a wide range of application. They are used in services which need support for authentication, identity, payment and other applications. Some of the applications which use smart cards are secure identity application, healthcare application, payment application and telecommunication application.

Smart card technology is currently recognized as most appropriate technology for identity applications. A lot of countries use smart card for citizen's personal ID, passports and for e-Government application. United States Department of Defense (DoD) Common Access Card (CAC) is one of the most advanced smart card ID program. Common Access Card serves as the DoD standard identification for active military personnel, reserve personnel, civilian employees and contractor personnel. It is the card used for access to DoD computers networks and system and will be used for physical access to DoD facilities.

Healthcare organizations are implementing smart health cards in order to support a variety of features and applications. Smart health cards can improve security and privacy of patient information. They can reduce healthcare fraud and provide secure carrier for portable medical record and improve exchange of medical record. Nowadays, medical identity theft is growing problem as the healthcare industry moves to electronic health records and health information exchanges. Smart health card provide strong identity management which can reduce number of medical identity theft.

In financial sector, both contact and contactless smart cards are used like credit and debit card. Number of merchant locations (restaurants, pharmacies, theatres, convenience stores) which accept contactless payment is increasing significantly. In electronic purse payment applications smart cards carries a stored monetary value. They are used to replace cash in frequent, low-value transactions such as paying for parking, public transport, internet etc

In telecommunications application smart cards are used for Subscriber Identity Module (SIM) and for Universal Integrated Circuit Card (UICC). SIM identifies and authenticates a subscriber to a wireless cell phone network. Subscriber can move his phone service to a new phone just by physically moving the SIM. It provides global roaming and access to voice, data and other services. Also, it can store contact information and phone numbers. UICC is a new generation of SIM which offers enhanced capabilities including better support for multiple applications and IP addressing. Smart cards are also used for pay phones systems instead of coins or magnetic card.

III. Electronic identification documents

Digital identity became a reality with electronic health cards, electronic driving licenses, e-Government services card, electronic personal ID cards and electronic passports. Types and standard of identification cards and review of using electronic identification documents are given in the next section. As an example, electronic passport based on ICAO (International Civil Aviation Organization) standard is described in last section.

III.1. Types and standards of identification cards

International standard ISO 7810 defines physical characteristics for identification cards. The standard defines four card sizes: ID-1, ID-2, ID-3 and ID-000. The dimensions of cards and usually usage are shown in the following table:

Format	***Dimension***	***Usage***
ID-1	85.60 × 53.98 mm	Most banking cards and ID cards
ID-2	105 × 74 mm	German ID cards issued prior to Nov 2010
ID-3	125 × 88 mm	Passports and visas
ID-000	25 × 15 mm	SIM cards

- The ID-1 format specifies a size of 85.60 × 53.98 mm. It is commonly used for banking cards (ATM cards, credit cards), driving licenses and personal identity cards and for passport cards in United States.
- The ID-2 format specifies a size of 105 × 74 mm. The ID-2 format is used by the German identity card issued until October 2010. Since November 2010, German ID cards are issued in the ID-1 format.
- ID-3 specifies a size of 125 × 88 mm. This format is used worldwide for passports and visas.
- ID-000 specifies a size of 25 mm × 15 mm. This format is used for SIM cards.

As it was mentioned, a lot of countries have already started to issue electronic documents for their citizens, which are based on digital certificates and smart cards. For example, ten European Union countries have already rolled out electronic ID cards and thirteen countries have committed to rolling out electronic ID cards. The overview of using electronic ID cards in Europe is given in the following table[65]:

Country	ID Card?	Primary ID?	eID card?	eID card
Austria	yes	no	yes	-
Belgium	yes	yes	yes	-
Bulgaria	yes	yes	no	-
Cyprus	yes	yes	no	no
Czech Republic	yes	yes	no	no
Denmark	no	-	no	no

[65] Table is taken from the website http://www.enisa.europa.eu. Data are from 2009.

Estonia	yes	yes	yes	-
Finland	yes	no	yes	-
France	yes	yes	no	yes
Germany	yes	yes	no	yes
Greece	yes	yes	no	no
Hungary	yes	no	no	yes
Ireland	no	-	no	no
Italy	yes	yes	yes	-
Latvia	no	-	-	yes
Lithuania	yes	yes	no	no
Luxembourg	yes	yes	no	yes
Malta	yes	yes	no	yes
Netherlands	yes	yes	yes	-
Poland	yes	yes	no	yes
Portugal	yes	yes	yes	-
Romania	yes	yes	no	yes
Slovakia	yes	yes	no	yes
Slovenia	yes	yes	no	yes
Spain	yes	yes	yes	-
Sweden	yes	no	yes	-
UK	yes	-	yes	-
Iceland	yes	yes	no	yes
Liechtenstein	yes	no	no	yes
Norway	no	-	-	no

European Union countries are good example of using electronic ID cards and applying them in e-Government services. However, there are some issues about cards interoperability between countries. In order to solve interoperability problems, 17 countries together with public and private sector established STORK (Secure idenTity acrOss boRders linKed) consortium. The primary goals of STORK are: access online Government service across Europe using national eID, better security of online transactions, using cross-border services over the Internet without the need to visit the country in advance, simplification of administrative formalities which will make it easier and cheaper to live and work in different European Union countries.

III.2. Electronic passport

Electronic passport technology has been developed after 2000 in order to increase security of travel documents and border processes. Today, almost all countries issue Machine Readable Passports (MRP) and about 90 countries issue electronic passports with chip or electronic Machine readable passports (eMRP). Machine Readable Passports have only Machine Readable Zone (MRZ) which can be read through optical recognition by reader. Both MRP and eMRP are Machine Readable Travel Documents (MRTD), but electronic passport has contactless smart card.

International Civil Aviation Organization (ICAO) standard 9303 defines characteristic of electronic passports. According to standard, electronic passport is a “Machine Readable Passport (MRP) containing a contactless integrated circuit (IC) chip within which is stored data from the MRP data page, a biometric measure of the passport holder and a security object to protect the data with Public Key Infrastructure (PKI) cryptographic technology”. All electronic passports shall carry symbol shown in figure 7.

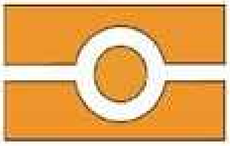


Figure 7

ICAO standard defines which data should be stored within contactless chip. They consist of 16 data groups (DG) and Document Security Object. Some of data groups are mandatory and some of them are optional. Data Group 1 (DG1) contains data from Machine Readable Zone. Standard takes in consideration three types of biometric identification system: facial recognition, fingerprint and iris recognition. Facial recognition is mandatory, while fingerprint and iris recognition are optional. Data Group 2 (DG2) contains facial recognition, Data Group 3 (DG3) contains fingerprint and Data Group 4 (DG4) contains iris recognition. The most important of the other groups is Data Group 15 (DG15) which provides support for active authentication and it is optional. Document Security Object (SO_D) contains signed hash values of all data group and it is mandatory. Therefore, there are 3 mandatory groups: DG1 with MRZ data, DG2 with fingerprint and SO_D.

Electronic passport use security mechanisms (passive authentication, active authentication and access control) to protect the authenticity (including integrity), originality, and confidentiality of the data stored on contactless chip. Security mechanisms and used cryptographic techniques are shown in following table:

Mechanism	**Protection**	**Cryptographic Technique**
Passive Authentication	Authenticity	Digital Signature
Active Authentication	Originality	Challenge-Response
Access control	Confidentiality	Authentication and Secure Channels

There are two generations of passport: eMRP 1G and eMRP 2G. eMRP 1G supports only passive authentication and Basic Access Control (BAC). eMRP 2G must have DG3 (fingerprint) or DG4 (iris recognition) and DG15 in order to support active authentication. Also, eMRP 2G use Extended Access Control (EAC). Within European Union deadline for implementation of 1G was 2006, and for implementation of 2G was 2009.

Passive authentication only verifies authenticity and integrity of data stored on the chip. Terminal (reader) verifies digital sign of the data groups. In order to verify digital sign, terminal have to read Document Security Object from chip and retrieve Document Signer Certificate, Country Signing CA Certificate and Certification Revocation List. Passive authentication does not prevent cloning of contactless chip.

Active authentication is security feature which prevent cloning of the chip. Chip has public key stored in DG 15 and corresponding private key stored in secure memory which may only be used internally. The chip can prove knowledge of private key in a challenge-response protocol. Terminal chooses random value and sends it to the chip. The chip digitally signs value and send to the terminal. The terminal recognizes that chip is genuine if the returned signature is correct. Active authentication does not provide confidentiality.

Access control may be basic and extended. Basic access control is used for less sensitive data (MRZ and facial image) and extended access control is used for sensitive data (fingerprint and iris recognition). Basic access control checks that the terminal has physical access to the document by requiring optically reading of MRZ zone. In this way, BAC prevents chip to be read without passport holder permission or knowledge. Extended access control introduce terminal authentication in order to provide confidentiality and also prevent cloning. Terminal has to have digital certificate issued by Country verifying CA of passport issuer country. Because of that, terminal must have certificates from Country verifying CA from all countries whose passports should be read.

Electronic passports have improved identity determination, but there are a lot of issues which should be solved. It is needed to strictly follow and implement standards in order to achieve full interoperability and use all capabilities which electronic passports offer.

CONCLUSIONS

Designing a new identity management system is complex and requires balance between security and privacy and the protection of personal information. The system must protect personal information at all times, while it is stored and while it is used. Security token must protect its content from being copied, altered and prevent unauthorized use, misuse, or disclosure of the personal information it carries. Exchange of data between identification card and reader or terminal must be protected to prevent unauthorized capture. Access to the personal information should be granted only after defined authentication process.

Due to its characteristics, only identity documents that use smart card technology have the strong security features that can improve privacy protection. Smart card technology provides an identity management system with the following advantages:

- Strong information protection. Smart cards can encrypt information stored on them and encrypt communication between card and reader.
- Strong ID security. Smart card chip has a variety of software and hardware capabilities which protect unauthorized access to stored information.
- Sophisticated "on-card" processing. On-card processing enables smart card to perform on-card functions (for example, encryption, decryption and other data processing) and to interact securely and intelligently with a card reader. Smart cards can securely store the biometric information and perform the comparison of the biometric inside the smart card chip to verify the individual's identity.
- Authenticated and authorized information access. Smart card can verify authenticity of the card reader and restrict access only to information required by that particular request.

Smart card technology is the most used identity management technology, especially for electronic identification documents like personal IDs, electronic passports and healthcare cards. However, there are many challenges in the implementation of smart card technology, particularly in terms of interoperability between different systems. These problems are likely to be solved thanks to the many initiatives and institutions working to resolve them.

GLOSSARY

ATM	Automated teller machine
BAC	Basic Access Control
CA	Certification authority
COS	Card operating system
CRL	Certificate revocation list
CSP	Cryptographic Service Provider
DSA	Digital signature algorithm
EAC	Extended Access Control
ECDSA	Elliptic Curve DSA
EEPROM	Electrically Erasable Programmable Read-Only Memory
EPROM	Erasable Programmable Read-Only Memory
GSM	Global System for Mobile Communications
IC	Integrated Circuit

ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Chip
IP	Internet protocol
ISO/IEC	International organization for standardization/International Electrotechnical Commission
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
MRP	Machine Readable Passport
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
MULTOS	Multi-Application Operating System for Smart Cards
PIN	Personal identification number
PKCS	Public Key Cryptography Standards
PKI	Public key infrastructure
RA	Registration authority
ROM	Read Only Memory
RSA	(Rivest, Shamir and Adleman) asymmetric encryption algorithm
SIM	Subscriber Identity Module
STORK	Secure idenTity acrOss boRders linKed
UICC	Universal Integrated Circuit Card
VPN	Virtual Private Network

REFERENCES

1. http://en.wikipedia.org/wiki/ISO/IEC_7810
2. http://en.wikipedia.org/wiki/ISO/IEC_7816
3. http://en.wikipedia.org/wiki/ISO/IEC_14443
4. http://www.icao.int
5. http://www.iso.org
6. http://www.smartcardbasics.com
7. http://www.smartcardalliance.org
8. http://www.eurosmart.com
9. http://www.enisa.europa.eu

INFORMATION WARFARE

Capt Daniel-Adrian MICU

INTRODUCTION

According to Wikipedia online encyclopedia, the term “Information Warfare” (IW) is primarily an American concept. This concept involves the use and management of information technology in order to have an advantage over the opponent. Information warfare may involve collection of tactical information, assurance(s) that someone's own information is valid, spreading of propaganda or disinformation to demoralize or manipulate the enemy and the public, undermining the quality of opposing force information and denial of information-collection opportunities to opposing forces[66]. Information warfare is very much connected to psychological warfare.

Along with the development of communication technologies, we can see that it had dramatically increased the way information is created, altered and transmitted to any party with the intent to influence the decision making. Because we are more exposed to sources of information, Information Warfare becomes a greater threat and weapon. Information can be both the target and the weapon. As a matter of fact, information may be the most formidable weapon of the 21st century. The more we are relying on sources of information through multiple distributors, the more we are exposed to information manipulation.

Nowadays, in our modern society, the processes of communication and information are relying on four critical infrastructures: the power grid, the communications infrastructure, the financial infrastructure, and the transportation infrastructure. Electricity and thus the *power grid* are the foundations of the entire system. Without electricity nothing works and we are back to using smoke signals. The *communications infrastructure* requires power and provides the ability to exchange information for news, business transactions, research, etc. The *financial infrastructure* requires power and communications and allows for the electronic flow of money. The *transportation infrastructure* (including the air traffic control system and the train routing systems) also requires power and communications infrastructures and allows for rapid and massive transportation of people and goods throughout the nation. A modern battle over the communications process involves all of these infrastructures. Information warfare now includes the electricity that powers our homes and hospitals, the phones, faxes, and computers that we and our government use in order to communicate and share information, and the trains and planes

[66] Wikipedia The Free Encyclopedia, http://en.wikipedia.org/wiki/Information_warfare, 05.06.2011, 19.00

that we use to get from one place to another. The new attention given to information warfare does not mark the birth of a new form of conflict, which some have implied. Rather, it marks a significant change in the implications of an old one.

I. WHAT IS INFORMATION WARFARE?

Winn Schwartau, expert on security, privacy, info war, cyber-terrorism and related topics, describes in his book *Information Warfare* three classes[67]: personal information warfare, corporate information warfare and global information warfare. What distinguishes the three categories is whether the subject of the attack is an individual, business enterprise, or government. The main concern in each of these levels is privacy, espionage, and terrorism. For an attacker at each one of these levels, stealing a personal identity, a corporate plan, or a national security secret would be immensely more profitable than just destroying that information.

I.1. PERSONAL INFORMATION WARFARE

This class refers to the attack against individual's privacy. As individuals, we have very little control over our private information. Our digital records and databases entries are more opened to information attacks because many of us aren't aware that our private information can be used by others in order to gain personal benefits, to use our identity and our connections to specific networks in order to get to the corporate level or even to global level. To blackmail someone, it is no longer necessary to survey him or her for a period of time. The same information can now be extracted with computer's help by monitoring electronic activity of the target, the email, messenger, social networks etc.

Because we are more and more relying on technology, we are more vulnerable in front of an attack. Along with convergence of technology come greater freedom and also greater threat. Along with the use of mobile devices, such as personal digital assistants and mobile phones, and internet enabled home devices, such as televisions and game consoles, there comes an increased opportunity for targeted attacks on individuals using cyberspace.

Everyday people are using computers without being aware of how easily they can fall victims to online identity theft. The attacker can use malicious software (malware) in order to illegally obtain someone's personal information; he can physically use a computer that was previously occupied by the victim and numerous other means to obtain what he is interested in.

[67] Reto E. Haeni - *Information Warfare - an introduction* , The George Washington University Cyberspace Policy Institute, January 1997, 06.06.2011, 08.05

I.2. CORPORATE INFORMATION WARFARE

Corporate information warfare refers to competition between corporations. But in our days we can call it “espionage” or even “war between corporations”. “The similarities between the military and business world grow each day. Both involve competition between adversaries with various assets, motives, and goals. Enemy surveillance and competitive intelligence are *de rigueur* in both fields”[68]. Because of the growing dependence of companies on sophisticated information systems, and because the rapid growth of Web-based electronic commerce, we can assume that information warfare theory will soon have a special place in leading business schools.

Companies are starting to include more computer security training and awareness than has been historically provided, in order to raise the interest for information security. Universities have started to incorporate computer ethics into both their computer science and business curriculums. News stories have been addressing security issues and the consequences of recent system penetrations with greater frequency and detail than ever before. Along with the growth of each of these trends, to disseminate information related to computer security and conflict, there will be added exposure to the computing populace of the ethical and very real consequences associated with subversions of computing security mechanisms and technologies.

In the United States more and more research is trying to find alternative measures in order to prevent an "electronic Pearl Harbor." One proposal assigns specific government agencies to be responsible for assisting various sectors in the American Information Infrastructure (which includes telecommunications, electric power, gas and oil, banking and finance, transportation, water, emergency services, and continuity of government related concerns and interests). The philosophies behind this approach is that national and economic security has become a shared responsibility between government and industry and that the federal government must collect appropriate information and share it with industry, while the private sector must take reasonable actions to protect itself from hackers[69].

In May 2011, security officials from Lockheed Martin announced that the US’s largest military contractor has battled disruptions in its computer networks that might be tied to a hacking attack on a vendor that supplies coded security tokens to millions of users[70]. That vendor was the RSA

[68] German, M., Donahue, D. A., and Schnaars, - *A chink in marketing’s armor: Strategy above tactics. Business Horizons* from http://indiana.edu/~tisj/readers/full-text/15-4%20cronin.pdf, 06.06.2011, 11.10

[69] Nitzberg, Sam - *Conflict and the Computer: Information Warfare and Related Ethical Issues* http://www.iwar.org.uk/iwar/resources/nitzberg/ethical.htm , 06.06.2011, 12.30

[70] Drew, Christopher, Markoff, John - *Data Breach at Security Firm Linked to Attack on Lockheed*, New York Times, http://www.nytimes.com/2011/05/28/business/28hack.html?_r=1 , 06.06.2011, 12.45

Security division of the EMC Corporation, which supplies the SecurID electronic tokens, used to gain access to computer networks by corporate employees and government officials from outside their offices.

RSA acknowledged in March that it had sustained a data breach that could have compromised some of its security products. Executives in the military industry said that Lockheed's problems appeared to be connected with that data breach and could be the first public signs of damage from it.

James A. Lewis, a senior fellow and a specialist in computer security issues at the Center for Strategic and International Studies, a policy group in Washington said that "The issue is whether all of the security controls are compromised". That's the assumption people are making."[71] In the light of recent events, the United States is warning that a cyber attack - presumably if it is devastating enough - could result in real - world military retaliation[72].

Officials say that every year, hackers steal enough data from U.S. government agencies, businesses and universities to fill the U.S. Library of Congress many times over.

I.3. GLOBAL INFORMATION WARFARE

This kind of war operates against industry, global economic forces and/or against states. Global IW is about not only stealing researcher's outcome and database's entries, but using this against the owners. It is hard to imagine the damage that can be done in global information warfare.

If someone, like a state, decides to invest millions of dollars in high technology used in global information warfare instead in buying airplanes, bombs and ammunition, in a couple of years it can be capable to affect the industry and even governments. With this kind of weapons someone can provoke the crash of Wall Street market or destroy a bank system.

At the beginning of 2003, the president of the U.S.A., George W. Bush, had approved the White House's National Strategy to Secure Cyberspace. He signed it nearly a week after the "Sapphire" Internet worm slowed Web traffic and disrupted bank cash machine services, airline flights and other critical parts of the Internet infrastructure[73].

"Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society – the federal government, state and local

[71] Ibidem , 06.06.2011, 13.05

[72] Stewart,Phil - *Analysis: Could a cyber war turn into a real one for the U.S.?,* Reuters, http://www.reuters.com/article/2011/06/01/us-usa-cyber-pentagon-idUSTRE74U75420110601, 06.06.2011, 13.15

[73] Krebs, Brian - *Bush Approves Cybersecurity Strategy*, Washington Post, http://www.securityfocus.com/news/2204, 06.06.2011, 20.30

government, the private sector and the American people" wrote Bush in a letter introducing the document.[74]

As I highlighted in Corporate IW about the Lockheed Martin case, the attack against an important company can have repercussions upon the information security of the state itself. Crashing a share market or destroying a bank system can lead to chaos not only in economy but in all areas of the state. Hacking a company's network that is responsible with supplying, among other, coded security tokens can have repercussions on long-term. Later, the attacker can gain access to governmental networks and will be able to alter, modify or steal sensitive information.

The most recent event is publishing by WikiLeaks submissions of private, secret, and classified media from anonymous news sources, new leaks and whistleblowers. Its website, launched in 2006 under the Sunshine Press organization, claimed to have a database of more than 1.2 million documents within a year of its launch[75]. WikiLeaks states that its "primary interest is in exposing oppressive regimes in Asia, the former Soviet bloc, Sub-Saharan Africa and the Middle East, but we also expect to be of assistance to people of all regions who wish to reveal unethical behavior in their governments and corporations." But in the same time, all that information disclosed can be used as a weapon. Where can we draw a line?

II. MEANS FOR ACCOMPLISHING INFORMATION ATTACK

II.1. OPERATIONS SECURITY (OPSEC)

Operations security (**OPSEC**) is a process that identifies critical information in order to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.[76]

The OPSEC process is most effective when it is fully integrated into all planning and operational processes. The OPSEC process involves five steps:

1. Identification of Critical Information: identifying the information that we need to protect;
2. Analysis of Threats: the research and analysis of intelligence, counterintelligence and open source information to identify possible adversaries to a planned operation;
3. Analysis of Vulnerabilities: examining each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then comparing those

[74] Lemos, Robert - *Bush unveils final cybersecurity plan*, CNET News, http://news.cnet.com/Bush-unveils-final-cybersecurity-plan/2100-1001_3-984697.html, 06.06.2011, 22.00

[75] Wikipedia The Free Encyclopedia, http://en.wikipedia.org/wiki/WikiLeaks, 06.06.2011, 23.50

[76] Wikipedia The Free Encyclopedia, http://en.wikipedia.org/wiki/Operations_security, 07.06.2011, 10.50

indicators with the adversary's intelligence collection capabilities identified in the previous action;

4. Assessment of Risk: first, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Second, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff;
5. Application of Appropriate OPSEC Measures: the command implements the OPSEC measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

Discussing unclassified information over the phone, leaving unclassified documents in a car, throwing them in the garbage, unclassified press release are not prohibited by security regulations. "Dumpster-diving"[77] is the number one means of gaining espionage information. Unclassified information of a sensitive nature, improperly handled, can easily provide adversaries with valuable information on current and future operations.

Insignificant pieces of information, to a trained adversary, can be like "pieces of a puzzle". Putting together those pieces, someone could obtain sensitive information. An adversary's agent, in charge with collecting information, frequently visit some of the same stores, clubs, recreational areas or places of worship. Determined individuals can easily collect data from cordless and cellular phones. Information that is not secret, like flight schedules, ship movements, temporary duty locations and installation activities, can be critical information.

It is important for one to know the adversary's capability. Knowing that, he can judge how and why the adversary may collect the information that he needs. Identifying what the adversary already knows helps one to prioritize his information.

OPSEC considers a variety of potential adversaries, ranging from the active (target or enemy or main competitor) to the passive (sympathizer or someone who supplies data to the active adversary) to the inadvertent (someone who accidentally gives away information).

In the OPSEC process, the third step is the analysis of vulnerabilities, direct and indirect, surrounding our operation. At this point, we look at how the activity *actually* works, rather than how people *think* it works. We study the chronology and timing of events, along with the flow of information, to ascertain which adversary would be interested in what data, and how he would be able to obtain them.

The manager then evaluates the **risk** to his or her operation or activity. The costs associated with fixing the vulnerability are weighed against the cost of the loss of the data, keeping in mind the

[77] Cox, Chris - *An Analysis of Dumpster Diving Law,* http://www.opsecprofessionals.org/articles/dumpsterdiving.html, 08.06.2011, 18.40

likelihood of our data being lost, as well as the impact such loss would have. The assessment of an adversary's capability includes not only his ability to collect the information, but also his capability to process and exploit (evaluate, analyse, interpret) in such a period of time so that he can use the information. In order to complete the risk assessment, it is necessary to combine this information. One method to reach a reasonable conclusion of the practicability of solution(s) might be to multiply the estimated loss in money*,* by the impact of risk, by the likelihood of risk. The solution, in money, must then be less expensive than the prejudice, in order to be feasible.

A countermeasure is anything that effectively obstructs an adversary's ability to exploit vulnerabilities. The most effective countermeasures are simple, straightforward, procedural adjustments that effectively eliminate or minimize the generation of indicators. Following a cost-benefit analysis, countermeasures are implemented in order to protect vulnerabilities that have the most impact on the project, as determined by the appropriate decision maker.

II.2. CONCEALMENT, COVER AND DECEPTION (CCD)

The information warfare has got a grown role nowadays because of the rapid penetration of information technologies to all spheres of human activities, including the military affairs. Most of the advanced world countries have increasingly focused on creating effective assets and methods of information warfare, which have a growing role in their efforts to gain success in the course of military operations. Military analysts believe that bringing directed information pressure upon the public and military administrative centres, the population and the armed forces of an unfriendly country can achieve their objectives quickly, effectively and sometimes even without war.

The information warfare is capable of making a profound change in the theory and practice of military art. It can also alter the views on the nature of confrontation between warring sides, along with its assets and methods. That brings forward the problem of preservation and protection of information, something that dictates the development of effective countermeasures capable of decreasing the enemy potential for penetration in our information webs (channels). One way of dealing with this task is to specify the place, the role and development priorities of what is known in Russian as "maskirovka"[78] - camouflage, concealment and deception (CC & D).

Deception and propaganda campaigns targeting the populations of developed countries, in a globalised and highly networked world, follow a different pattern, but also exploit classical deception technique. The principal distinction in application is a result of the lack of structural

[78] A N Limno & M F Krysanov - *Information warfare and camouflage, concealment and deception*, http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&folder=66&paper=1257, 08.06.2011, 21.40

control over global media organizations and networks, which are not part of the regime or movement's internal organization. The result of this is that media organizations must be subjected to a deception effort designed to compel them to become a delivery mechanism for deceptive messages targeting the victim population. Most modern electronic and print media organizations are primarily focused on the delivery of information rather than dedicated news and news analysis. Because of that, the depth of analysis or accuracy of the material has no primary role in media organizations.

This is a product in dynamics of a commercial market, in which competing media players must attract the interest of viewers in order to achieve favorable ratings and thus attract subscriptions or advertising revenues. In a sense, this is a commercial application of Goebbels' view. He realized that, for instance, in cinematic propaganda, the viewers should be entertained; entertaining programs should sustain the listener's attention. The radio was created to be a one-way conduit of (mis)information from the party to population, and also to provide light entertainment and news that the party deemed accessible for public consumption. Propaganda should be popular, not intellectually pleasing[79].

In terms of the Information Warfare strategies, the play by media organizations is a compound strategy of degradation and corruption, centered on audience interests and prejudices, aiming to maximum audience visitation rates at the expense of competitors.

A regime or political movement, intending to target an audience on the global stage, can only be successful if it is able to wrap its deceptive message in an envelope of material which is attractive to global media organizations. As a result, the deceptive message must provide content which is dramatic, violent, intensely controversial, or any combination of the three and which appeals to the prejudices of the target population in the deception game.

One example is South East Asian conflict. North Vietnam used the mass media against global, and especially the US population, to deliver deceptive propaganda. This campaign was successful because media’s self interest enabled its use. US consumers, via advertising revenue to media, funded the distribution of deceptive propaganda which destroyed public support for the war and led to a US withdrawal.

A more recent example is the ongoing campaign of kidnappings, suicide bombings, roadside bombings and assassinations in Muslim nations, the recent public transport bombings in Spain and the UK, and the September 11 attacks in the US. No differently than during the South

[79] Hill, Andy - *A Closer Look at Nazi Propaganda*, http://hubpages.com/hub/A-Closer-Look-at-Nazi-Propaganda, 09.06.2011, 09.30

East Asian conflict, global consumers are funding the distribution of deceptive propaganda via media organizations.

Haswell defined five deception techniques[80]:

1. **The Lure** – this technique presents the opponent with a sudden advantage they may exploit. The victim perceives an advantageous situation which has been fabricated to weaken their position. At the most basic level, this play qualifies as an example of the corruption strategy, as mimicry is employed to create a perception of an advantageous situation which does not exist. As a supporting strategy could be Degradation, by using camouflage techniques to hide information which may expose the strategy.
2. **The Repetitive Process** – this technique conditions the opponent by repetition to accept harmless behavior that is used as a cover for ulterior operations. It is similar to the Lure in having the same compound and canonical forms. Its implementation differs as it is intended to deceive by mimicking behaviors which are not characteristic of preparations for an attack. The aim of the Repetitive Process is different from the Lure, since the latter is designed to compel an opponent to make a move in the game, whereas the former is intended to conceal preparations for a move by the attacker.
3. **The Unintentional Mistake** – this technique leads an opponent to believe that valuable information has come into his hands by mistake, for instance by negligence or incompetence. It is a mimicking technique and thus also qualifies as corruption. The player mimics a mistake and the victim is compelled to exploit the mistake. More than often this play will include concealment or camouflage as a supporting strategy, and thus exists in both canonical and compound forms.

Some case studies show the use of the Unintentional Mistake as a technique used to introduce a false belief that intelligence sources being used by the victim are in fact double agents, when this is not so. As a result the victim will destroy its intelligence network in an effort to remove the believed to be compromised agents. If the Unintentional Mistake is used for this purpose, it is part of a larger compound strategy, in which corruption and degradation are used as supporting strategies for a denial game, in which the victim is subverted into using internal resources to self destruct.

4. **The Obvious Solution** – this technique provides deceptive information to support the idea that the obvious method will be used, while hiding information related to the actual method. It is an example of corruption and degradation, in that mimicry or concealment will be employed to hide the real intent from a victim. It aims to reinforce an existing but incorrect perception by

[80] C. Kopp - *Classical Deception Techniques and Perception Management vs. the Four Strategies of Information Warfare*, http://www.csse.monash.edu.au/publications/2005/IWAR05-Kopp.pdf, 08.06.2011, 20.50

the victim that the obvious play is the correct play. Whereas earlier plays either aim to implant a false perception or aim to conceal, the Obvious Solution is mostly intended to reinforce an existing but incorrect perception by the victim. Knowledge of the victim's actual perception is often valuable if this play is to be implemented.

5. **The Piece of Bad Luck** – this technique is similar to the Unintentional Mistake, except the bad luck cannot be attributed to anyone. It is a form of the Unintentional Mistake and thus a canonical or compound strategy using corruption and degradation. The implied cause of the "unintended" disclosure is different.

II.3. PSYCHOLOGICAL OPERATIONS (PSYOPS)

Psychological operations are planned operations that transmit selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.[81]

The nature of PSYOPS is in continuous change. PSYOPS personnel must bear a large range of missions and forced structures depending on the environments, from austere to highly sophisticated. PSYOPS are planned, coordinated and executed before, during and after conflicts, and must be integrated at all echelons in order to achieve its full potential. PSYOPS are conducted at strategic, operational and tactical levels of war to influence foreign audiences.

Alexander the Great perfected a method of psychological harassment, which was the hidden cause of many of his victories. He developed psychological procedures and his actions were similar to modern-day psychological operations. He developed the following practices:

- Maintain good relations with pacifist elements within neighboring people in order to take advantage of favorable opinions and sentiments;
- Use secret agents to infiltrate and spread rumors and news;
- In moments of crisis, bury the enemy — with public opinion — under an avalanche of information, true or false, that can produce concern, demoralization and chaos.

Genghis Khan was leading huge hordes of savage horsemen across Russia and into Europe. Agents, planted in advance to spread rumors and other forms of propaganda, exaggerated the size of his army. To supplement his PSYOPS activities, Genghis Khan also used rapid troop maneuvers to confirm the illusion of invincible numbers. Since the Mongols created an image of total barbaric domination, target groups never believed they were the victims of psychological warfare.

[81] Wikipedia The Free Encyclopedia, http://en.wikipedia.org/wiki/Psychological_Operations_(United_States), 09.06.2011, 10.30

Other than the above, there are numerous examples in recent times where in the application of PSYOPS has been a key winning factor, including the current war in Iraq. During the Second World War, all sides made extensive use of PSYOPS. The 'Tokyo Rose' of Japan and 'Axis Sally' of Germany are well remembered by veterans. The subtleties of these radio programs remain unmatched till date. Even the BBC had the most innovative use of PSYOPS when they broadcast English language lessons for the Germans.

According to the Field Manual of US Army concerning psychological operations, PSYOPS soldiers perform the following five principal missions[82] to meet the intent of the supported commander:

- *Advise the commander* on Psychological Operations actions, PSYOPS enabling actions, and targeting restrictions that the military force will execute. These actions and restrictions minimize adverse impacts and unintended consequences, attack the enemy's will to resist, and enhance successful mission accomplishment.
- *Influence foreign populations* by expressing information subjectively to influence attitudes and behavior, and to obtain compliance or noninterference. These actions facilitate military operations and minimize unnecessary loss of life and collateral damage.
- *Provide public information* to foreign populations to support humanitarian activities, restore or reinforce legitimacy, ease suffering, and maintain or restore civil order.
- *Serve as the supported commander's voice* to foreign populations to convey intent and establish credibility.
- *Counter enemy propaganda, misinformation, disinformation, and opposing information* to portray friendly intent and actions correctly and positively, thus denying others the ability to polarize public opinion and political will against our forces.

When properly employed, PSYOPS can save lives of friendly and/or adversary forces by reducing adversary's will to fight. By lowering adversary morale and reducing their efficiency, PSYOPS can also discourage aggressive actions and create dissidence and disaffection within their ranks, ultimately inducing surrender.

According to Doctrine for Joint Psychological Operations, PSYOPS are conducted at three levels[83]:

- **Strategic-level:** PSYOPS are used in order to influence foreign attitudes, perceptions, and behavior in favor of the goals and objectives. These activities predominantly take place outside the military arena but can receive support from military PSYOPS forces.

[82] *Psychological Operations Tactics, Techniques, and Procedures*, Field Manual No. 3-05.301, http://www.fas.org/irp/doddir/army/fm3-05-301.pdf, 09.08.2011, 12.00

[83] *Doctrine for Joint Psychological Operations*, Joint Publication 3-53, 5 September 2003, http://www.iwar.org.uk/psyops/resources/doctrine/psyop-jp-3-53.pdf, 09.06.2011, 18.30

Strategic PSYOPS play an important role in theater security cooperation (TSC) agreements.

- **Operational-level:** PSYOPS are designed to strengthen capabilities to conduct military operations in the operational area and accomplish particular missions across the range of military operations. Along with other military operations, PSYOPS may be used independently or as an integral part of other operations throughout the operational area. Operational-level PSYOPS also play an important role in supporting military-to-military programs as part of TSC agreements. These initiatives have promoted military professionalization and human rights programs within host nation militaries, as well as many other programs designed to improve civil-military relations.
- **Tactical-level:** PSYOPS outline how military force will be employed against opposing forces to attain tactical objectives. PSYOPS are conducted as an integral part of multinational, joint, and single-Service operations.

One example of Joint Psychological Operations is NATO campaign in former Yugoslavia. During the 78-day bombing campaign, a total of 104.5 million leaflets were dropped over Belgrade, Kosovo and other major urban and rural areas throughout the country[84]. The thousands of Yugoslav Federal Army soldiers within Kosovo, as well as the civilian population throughout Serbia, were routinely targeted by PSYOPS products. In addition to the millions of leaflets dropped, thousands of posters, handbills and newspapers were also produced by tactical PSYOPS forces in Albania. From the refugee camps in Albania and Macedonia to the citizens of Belgrade and Kosovo, PSYOPS products were widely disseminated to inform and influence the Serbian and Albanian populations.

II.4. PHYSICAL DESTRUCTION

In combat operations, the commander accomplishes the mission through the application of lethal combat power. He uses Information Operations to disrupt or destroy enemy information systems, primarily through Electronic Warfare and physical destruction. Physical destruction is the most effective mean for preventing the enemy to use his command and control systems and achieving an information advantage in the application of force. In peace operations, however, the principle of restraint and the neutrality of the peace operations force mean that lethal power is rarely the mean to mission accomplishment.

Clausewitz believed that combat and bloodshed were an integral part of warfare. “Kind-hearted people might of course think there was some ingenious way to disarm or defeat and enemy without too much bloodshed, and might imagine this is the true goal of the art of war. Pleasant as

[84] Ibidem, 09.06.2011, 19.25

it sounds, it is a fallacy that must be exposed"[85]. Do we like it or not, physical destruction is playing its role in information warfare. One of the important parts of information warfare is infrastructure warfare, in which the infrastructure of an enemy is targeted with both "regular" technology (bombs, missiles, troops on the ground) and "information" technology. The attempt to utilize malicious software to disrupt and alter enemy telecommunications without physical destruction and to induce a psychological state in the enemy will lead him to "do your will".

The goal of information warfare is to disrupt, disable, destroy, or modify an adversary's information and information systems while simultaneously protecting your own. While electronic attacks of a network via computer and modem are the "cleanest" means of information warfare, physical attacks on the network's infrastructure are also possible and should always be considered as an option open to terrorists.

Physical destruction operations in peace operations focus on the neutralization of adversary capabilities. In determining whether or not physical destruction operations apply, the Information Operations planner must identify the adversary's means to asses the situation, and then target those means for neutralization. Tactics employed to neutralize the adversary's ability to asses the situation or exercise command and control include[86]:

- Occupying or controlling access to facilities used by the adversary for command, control and communication and early warning;
- Shutting down power sources for command, control and communication and early warning systems;
- Delaying groups or individuals of the adversary's support base attempting to mass;
- Arresting or detaining key individuals and instigators of the adversary support base to prevent them from provoking disturbance at "hot spots".

Physical occupation or controlling access of adversary command, control and communication and early warning facilities is a mean of temporarily preventing the adversary from using those capabilities. If the peace operation force cannot occupy the facility or control access to it, cutting off its power may provide a less-intrusive means of temporarily depriving the adversary use of the facility's functions. Examples of command, control and communication and early warning facilities that could possibly be targeted for physical destruction include: TV and radio transmitting towers and stations, police stations, air raid sirens, and radio frequencies used to transmit radio or telephone communications.

[85] Matthew J. Littleton - *Information Age Terrorism: Toward Cyberterror*, http://www.fas.org/irp/threat/cyber/docs/npgs/ch2.htm#note11, 09.06.2011, 20.20

[86] Arthur N. Tulak - *The Physical Destruction Component of Information Operations in Peace Enforcement*, http://www.iwar.org.uk/iwar/resources/call/tulak.htm, 09.06.2011, 21.00

II.5. ELECTRONIC WARFARE (EW)

For a long time, electronic warfare has been a separate subject from computer security, even though they have some common technologies (such as cryptography). This is starting to change as elements of the two disciplines fuse to form the new subject of information warfare. The military's embrace of information warfare as a slogan over the last years of the twentieth century has established its importance.

The goal of electronic warfare is to control the electromagnetic spectrum. It is generally considered to consist of[87]:

- **Electronic attack**, such as jamming enemy communications or radar, and disrupting enemy equipment using high-power microwaves;
- **Electronic protection**, which ranges from designing systems resistant to jamming, through hardening equipment to resist high-power microwave attack, to the destruction of enemy jammers using anti-radiation missiles;
- **Electronic support** which supplies the necessary intelligence and threat recognition to allow effective attack and protection. It allows commanders to search for, identify and locate sources of intentional and unintentional electromagnetic energy.

Electronic attack prevents or reduces an enemy's use of the electromagnetic spectrum. It can be accomplished through detection, denial, disruption, deception, and destruction. Electronic attack includes direct attack with high-speed antiradiation missiles (HARMs) and active applications such as decoys, noise jamming, deceptive jamming, and expendable miniature jamming decoys.

High power electromagnetic energy can be used as a tool to overload or disrupt the electrical circuitry of almost any equipment that uses transistors, micro-circuits, or metal wiring. Directed energy weapons amplify or disrupt the power of an electromagnetic field by projecting enough energy to overheat and permanently damage circuitry, or jam, overpower, and misdirect the processing in computerized systems.

Electromagnetic jamming and the suppression of enemy air defenses are also applications of electronic attack[88]. Jamming enemy sensor systems can limit enemy access to information on friendly force movements and composition and can cause confusion. Jamming can degrade the enemy's decision making and implementation process when applied against command and control systems. An adversary heavily dependent on centralized control and execution for force employment presents an opportunity for electronic attack. The goal of suppression of enemy air

[87] T. Hobbes - *Electronic and Information Warfare*, http://www.cl.cam.ac.uk/~rja14/Papers/SE-16.pdf, 09.06.2011, 21.30

[88] Air Force Doctrine Document 2-5.1, *Electronic Warfare*, http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5_1.pdf, 09.06.2011, 22.30

defenses operations is to provide a favorable situation in which friendly tactical forces can perform their missions effectively without interference from enemy air defenses.

Electronic protection is part of defensive counter information and needs to be properly integrated into the information operations plan. Friendly force reliance on advanced technology demands comprehensive electronic protection safeguards and considerations. Proper frequency management is a key element in preventing adverse effects by friendly forces. Much of the success of electronic protection occurs during the design and acquisition of equipment.

Another way to ensure an active electronic protection is by using cryptography. Cryptography can be defined as the conversion of data into a scrambled code that can be deciphered and sent across a public or private network. Decoding computer-generated messages is fast becoming impossible. The combination of technologies such as the triple- digital encryption standard (DES) for message communication using private keys, and public key encryption (PKE) for passing private keys using public keys (so set up communications remain in the clear) will probably overwhelm the best code-breaking computers.

There are three main forms of encryption:

- **Bulk encryption**: encryption of all data on a link on which transmission is continuous. It is preventing unauthorized reception and traffic analysing. This form of encryption protects against interception and deception.
- **Message encryption**: both header and content of a message in encrypted. It doesn’t prevent traffic analysing and it doesn’t protect against deception because someone can delay the replay of previous traffic.
- **Message-content encryption**: only the bodies of messages are encrypted, leaving message headers in plain text. This form of encryption is often used in packet-switching systems, so intermediate switches and routers don’t need attached cipher devices. This form of encryption doesn’t protect against deception because someone can delay the replay of previous traffic.

A system that provides encryption and decryption is referred to as a ***cryptosystem*** and can be created through hardware components or program code in an application. The cryptosystem uses an encryption algorithm, which determines how simple or complex the process will be. Most algorithms are complex mathematical formulas that are applied in a specific sequence to the plaintext. Most encryption methods use a secret value called a key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the text Cryptosystems can provide confidentiality, authenticity, integrity, and nonrepudiation services. It does not provide availability of data or systems. ***Confidentiality*** means that unauthorized parties cannot access information. ***Authenticity*** refers to validating the source of the message to ensure the sender is properly identified. ***Integrity*** provides assurance that the message was not modified during transmission, accidentally or intentionally. ***Nonrepudiation*** means that a sender cannot deny sending the message at a later date, and the receiver cannot deny receiving it. Someone can't alter the message before it arrived to your computer and no one else was able to read this message as it traveled over the network.

Commanders, aircrews, and operators use **electronic support** to provide near-real-time information to supplement information from other intelligence sources. Additionally, electronic support information can be correlated with other ISR information to provide a more accurate picture of the battle space. This information can be developed into an electronic order of battle for situational awareness and may be used to develop new countermeasures.

CONCLUSIONS

Information warfare can be found at any level: starting from personal level and continuing at the corporate level and global level. We can find it in every aspect of our life. We are more and more relying on technology, and because of that we are daily bombed with information through every channel. We are relying on television in order to receive information about our society and about the world. We are relying on internet, using it to communicate with other people and to search information that is useful to us.

Corporate information warfare is used every day in our society. Only a small part of all incidents are known. Many incidents are never discovered and most others are not known outside of the organization for fear of negative reactions.

Our systems are mainly vulnerable for the following reasons: high tech equipment is available all over the world (for friend and enemy); the awareness of the danger of Information Warfare is mostly not appropriate at the executive level; a lot of computer systems are poorly managed and poorly equipped to prevent against intruders; attackers use sophisticated tools to break into systems or get desired information; attacks over the Internet can originate from places that are physically located on the other side of the globe; it is impossible to make a system absolutely secure.

The high tech societies are especially vulnerable to information warfare attacks. They rely heavily on today's electronic communication and data exchange. An offender can attack these information backbones with low investment of finance and equipment in comparison to the damage. In the world today information warfare is an industry in which is invested billions of dollars annually.

Information warfare will be the war of the future between states high technological developed. And because of that, it is clear that the security of information systems must be a high priority for any company or state.

REFERENCES

1. Air Force Doctrine Document 2-5.1 - *Electronic Warfare*, http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5_1.pdf , 5 November 2002
2. Cox, Chris - *An Analysis of Dumpster Diving Law,* http://www.opsecprofessionals.org/articles/dumpsterdiving.html, 2008
3. Drew, Christopher, Markoff, John - *Data Breach at Security Firm Linked to Attack on Lockheed*, New York Times, http://www.nytimes.com/2011/05/28/business/28hack.html?_r=1, 27 May 2011
4. *Doctrine for Joint Psychological Operations*, Joint Publication 3-53, http://www.iwar.org.uk/psyops/resources/doctrine/psyop-jp-3-53.pdf, 5 September 2003
5. German, M., Donahue, D. A., and Schnaars, - *A chink in marketing's armor: Strategy above tactics. Business Horizons* from http://indiana.edu/~tisj/readers/full-text/15-4%20cronin.pdf
6. Hill, Andy - *A Closer Look at Nazi Propaganda*, http://hubpages.com/hub/A-Closer-Look-at-Nazi-Propaganda
7. Hobbes, T. - *Electronic and Information Warfare*, http://www.cl.cam.ac.uk/~rja14/Papers/SE-16.pdf
8. Krebs, Brian - *Bush Approves Cybersecurity Strategy*, Washington Post, http://www.securityfocus.com/news/2204, 31 January 2003
9. Kopp, C. - *Classical Deception Techniques and Perception Management vs. the Four Strategies of Information Warfare*, http://www.csse.monash.edu.au/publications/2005/IWAR05-Kopp.pdf
10. Lemos, Robert - *Bush unveils final cybersecurity plan*, CNET News, http://news.cnet.com/Bush-unveils-final-cybersecurity-plan/2100-1001_3-984697.html, 14 February 2003
11. Limno, A.N., Krysanov, M.F. - *Information warfare and camouflage, concealment and deception*, http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&folder=66&paper=1257, March-April 2003
12. Littleton, Matthew J. - *Information Age Terrorism: Toward Cyberterror*, http://www.fas.org/irp/threat/cyber/docs/npgs/ch2.htm#note11

13. Nitzberg, Sam - *Conflict and the Computer: Information Warfare and Related Ethical Issues,* http://www.iwar.org.uk/iwar/resources/nitzberg/ethical.htm
14. *Psychological Operations Tactics, Techniques, and Procedures*, Field Manual No. 3-05.301, http://www.fas.org/irp/doddir/army/fm3-05-301.pdf, December 2003
15. Reto E. Haeni - *Information Warfare - an introduction*, The George Washington University Cyberspace Policy Institute, January 1997, http://docs.google.com/viewer?a=v&q=cache:r0PzdZk0IucJ:citeseerx.ist.psu.edu/viewdoc/download?doi%3D10.1.1.147.5267%26rep%3Drep1%26type%3Dpdf+15.+Reto+E.+Haeni+-+Information+Warfare+-+an+introduction,+The+George+Washington+University+Cyberspace+Policy+Institute,+January+1997&hl=ro&gl=ro&pid=bl&srcid=ADGEESjF1_Fdpd42hPofh5-QhdbaRHWol4Z5uJaxgyqYS7SDrz8-RqW7tgQQ1en5vHCAzhibQcVfnGKzIyW4yvNTTvlbThbaFY7ATNpeWWfT1GccCRF5RqXpFPkoygQVh_-6m-2nd9HS&sig=AHIEtbQRpoaRqK2jJOaDeddTa2ODGGbGpQ
16. Stewart, Phil - *Analysis: Could a cyber war turn into a real one for the U.S.?,* Reuters, http://www.reuters.com/article/2011/06/01/us-usa-cyber-pentagon-idUSTRE74U75420110601, 1st of June 2011
17. Tulak, Arthur N. - *The Physical Destruction Component of Information Operations in Peace Enforcement*, *http://www.iwar.org.uk/iwar/resources/call/tulak.htm*
18. Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/.

THE ROMANIAN NATIONAL STRATEGY AND KEY POLICY MEASURES IN THE DOMAIN OF NETWORK AND INFORMATION SECURITY

Cmd. Valeriu ANTON

INTRODUCTION

„Sean McGurk, director of the Control Systems Security Program in the Department of Homeland Security (DHS) National Cyber Security Division (NCSD), reported that Einstein 2, the federal government's network intrusion detection system, registered a total of 5.4 million "hits" in 2010, an average of 450,000 hits per month and 15,000 per day.

Einstein 2 has so far been deployed at 15 of the 19 large federal departments and agencies that maintain their own locations for the Trusted Internet Connections (TIC) initiative, which is designed to consolidate the number of external internet connections at federal agencies.

McGurk explained that Einstein's next-generation, Einstein 3, will be able to "automatically detect and disrupt malicious activity before harm is done to critical networks and systems" in addition to detecting that activity. The system recently was successfully tested by the DHS and the National Security Agency during the Comprehensive National Cybersecurity Initiative 3 Exercise"[89].

Fortunately, these attacks are happening in United States of America, the most developed country in the world. Romania is a beginner is implementation of eGovernment and eSociety. In this paper I will try to present a short overview of the legislative framework, the authorities which are involved, and facts, trends and good practices in the field of information security.

I. NIS[90] NATIONAL STRATEGY, LEGISLATIVE FRAMEWORK AND KEY POLICY MEASURES

I.1. Overview of the NIS national strategy

Both Romanian Government programmes 2004-2008, and 2009-2012 under the sections regarding informational society, a series of specific objectives and measures are included, with relevance on the domain of network and information security:

- Extending the broadband informational infrastructure for local communities;

[89] http://www.infosecurity-us.com/view/18274/federal-networks-attacked-15000-per-day-in-2010-says-dhs-official/

[90] Network and Information Security

- Development of the national e-Romania platform and National Electronic System (SEN) by integrating news electronics services in order to raise the access level of population at informational public services;
- Increasing the informational security level of public networks using CERT[91];
- Promoting measures that will allow the improvement of IT indicators, will make flexible the structures of central and local administration for the initiation, sustaining and starting IT projects by the small and medium sized enterprises, as well as open some programs of financing the projects in cooperation with internal and international institutions.

The **eGovernment** has been actively promoted in the last years, being considered as the best way of organising public management in order to increase efficiency, transparency, accessibility and responsiveness to citizens, while reducing bureaucracy and corruption.

IT strategy of the Ministry of Communications and Information Society

The mission of the **Ministry of Communications and Information Society (MCIS)** is to create solid premises that will ensure the transition to the Information Society in Romania. The Information Society is an objective of the development of the country and not a desideratum in itself.

MCIS is managing the following relevant NIS Romanian national strategies[92]:

- The Romanian national strategy for development of the broadband eCommunications 2009-2015;
- The strategy for the universal service;
- The strategy for the transition from analogue to digital television and for digital multimedia services;
- National-wide guidance for public authorities for managing their web sites;
- Electronic signature;
- Electronic archiving, etc.

I.2. The legislative framework

The Romanian Government has dedicated a lot of effort in recent years to develop a legal framework favouring the development of the Information Society and eGovernment. This framework includes:

- Law on Electronic Signature (2001):

[91] Computer Emergency Response Team (Centru de reacție și răspuns la incidentele de securitate informatică)

[92] We *refer to the strategy documents published on the website of the Ministry (only in Romanian):* *http://www.mcsi.ro/Minister/Domenii-de-activitate-ale-MCSI/Comunicatii-electronice/Strategii*

  - Ministry of Communications and Information Society (MCIS) is the authority in charge of the regulation of eSignatures;
  - defines the procedure for approving, delaying and recalling the decision of accreditation of the certification services providers;
- Law on Free Access to Information of Public Interest (2001);
- Law on the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data (2001);
  - regards automatic processing of personal data, referring to control authorities and cross-border data flow;
- Law on Electronic Commerce (2002):
  - defines eCommerce and other basic concepts, such as electronic messaging or exchange of data over the Internet;
  - stipulates heavy punishments for the possession of equipments for falsifying electronic payments instruments;
  - establishes who can start an eBusiness registered in Romania and how.
- Law regarding the electronic payment of local taxes (2002):
  - allows for the electronic payment of fines, taxes and other fiscal obligations;
- Law regarding the Universal Service and the Users' Right (2003);
- Law on the processing of personal data and the protection of privacy in the electronic communications sector (2004);
- Ordinance concerning the award of public contracts, public works concession contracts and services concession contracts (2006).

Moreover, Romania was the first country in Europe to transpose the European Union regulatory framework for eCommunications into national legislation, between 2002 and 2003.

Other department regulations

Department regulations are effective in the domain of responsibility of their respective issuing authority. The following department regulations have relevance and applicability in the domain of network and information security:

- Regulations of the National Authority for Communications (ANCOM);
- ORNISS directives: national classified information; NATO classified information; EU classified information;
- Orders of the Ministry of Internal Affairs;
- Romanian Intelligence Service recommendations;
- Foreign Intelligence Service recommendations;

- Special Telecommunications Service recommendations;
- Ministry of Justice recommendations;
- Ministry of Defense recommendations;
- Provisions of National Bank of Romania;

Cybercrime

Computer crimes covered by the Romanian Anti-corruption Law

Several articles of the Romanian Anti-corruption Law are of relevance in the NIS context, as they directly address the computer misuse and the unlawful access to, or use of, information..

The most relevant computer-related illegal acts addressed relate to acts that involve:

- illegal access to data;
- illegal transmitting, altering, deleting or deteriorating computer data;
- the production, sale, import, distribution of a device or a computer programme designed to be used for illegal purposes.

The Service for Combating Cybercrime under the Romanian Directorate for Investigating Organised Crime and Terrorism Offences of the Prosecutor‘s Office of the High Court of Cassation and Justice (DIICOT) is the competent Romanian Authority in enforcing the legal measures against the cybercrime.

II. OVERVIEW OF THE NATIONAL eGOVERNMENT AUTHORITIES

Ministry of Communications and Information Society (MCSI)

The Ministry of Communications and Information Society is the main policy and strategy provider for eGovernment in Romania. As the specialised body of central public administration in the ICT sector, it was established in 2001 with the objective of implementing the Romanian Government's policy in this field. It is responsible for defining the restructuring policies, coordinating the privatisation process in the ICT sector, financing the main projects to make the transition of the Romanian society to an Information Society and promoting the development of the Internet. Moreover, the MCSI is in charge of the harmonisation of relevant legislation to the European Union's provision.

National Centre for Management of Information Society (CNMSI)

The National Centre for Management of Information Society (CNMSI) is a public institution and a legal entity, with the main tasks of coordinating and implementing all operating systems that are related to the provision of eGovernment services. The new agency has been bestowed with two main responsibilities in relation to coordination:

- the administration and operation of:
  - the eGovernment Portal (also known as National Electronic System - SEN) e-guvernare.ro;
  - the Electronic System for Public Procurement e-licitatie.ro;
  - the Virtual Payment Desk www.ghiseul.ro
  - the IT System for the Electronic Attribution of International Authorisations on Transport Goods autorizatiiauto.ro.
- the regulation of specific activities according to law.

National Centre "Digital Romania" (CNRD)

CNRD has as main tasks the management, coordination and operation of information systems through which electronic public services are provided within the eRomania Programme and the implementation, operation and management of the project 'Electronic Point of Single Contact' under the Services Directive and Law no. 49/2009. Using this website public administration seeks to become more efficient by simplifying the procedures applicable to services and service providers in order to achieve an interoperable platform at the national and European levels.

Ministry of Administration and Interior (MAI)

The Ministry of Administration and Interior is the actor that mainly uses eGovernment services in the country. Furthermore, it is in itself a policy contributor in the field.

National Institute for Research and Development in Informatics (ICI)

ICI is Romania's main research institute in the field of ICT. The main activities of the institute in relation to eGovernment coordination focus on:

- application of research projects developed by national authorities and programmes financed by European funds;
- assessment of IT projects;
- monitoring / auditing scientific and technical activities for implementation of ICT projects;
- feasibility studies for computerization projects in national institutions and agencies;
- study and research in ICT;
- development of information security services and networks;
- assessment of on-line services.

National Authority for Management and Regulation in Communications of Romania (ANCOM)

On 19 March 2009, ANC was reorganised as the National Authority for Management and Regulation in Communications (ANCOM). ANCOM is the unique administrator of policies in the field of electronic communications and information technology. In more detail, ANCOM took the role of national administration of the Top Level Domain (TLD), ".ro", and the Second Level Domain (SLD), ".eu" for the domain names reserved for Romania and became the unique administrator of the policies in the field of electronic communications and information technology. However, granting of domain names is still exercised by the National Institute for Research and Development in Informatics (ICI). Previously, ANC was established in September 2008 through the reorganisation of both the National Regulatory Authority for Communications and Information Technology (ANRCTI, which was dissolved in the same month) and the National Institute of Research and Development in Informatics (ICI).

Association for Electronic Payments in Romania (APERO)

APERO was established in January 2008, by a court decision and it now enumerates 28 members spreading electronic payments within the country. In 2010 it launched, in co-operation with the National Centre for the Management of Information Society (CNMSI), the National Information System for Tax Payment Online. This project is promoted by the Ministry of Telecommunications and Information Society (MCSI) with the view to facilitate taxpayers accomplishing their transactions swiftly and at a minimum cost.

Security Incidents Response and Expertise Centre (CERIS)

CERIS, which operates within the Ministry of Communications and Information Society, is in charge of promoting the information security culture within Public Administration organizations. Among other activities, CERIS provides the following services to the Romanian administration: formulating recommendations on means to protect IT systems against potential security problems by anticipating incidents and ensuring fast solving of issues; providing information on the security of IT systems; guiding the administration in increasing its IT systems' security and in managing security incidents resulting from vulnerable exploitations.

National Supervisory Authority for Personal Data Processing

Created in 2005, this independent public body supervises and controls the legality of personal data processing falling under the personal data protection legislation. All of the data protection files previously kept by the Ombudsman have been handed over to the Authority. The competences of the Authority are those of a control institution, including the investigation of personal data processing - conducted under Law no.677/2001 - and the sanctioning - in case legal provisions were infringed by the personal data processors as a result of self-notification, or based on complaints filed by the person whose rights were infringed.

III. NIS FACTS, TRENDS AND GOOD PRACTICES

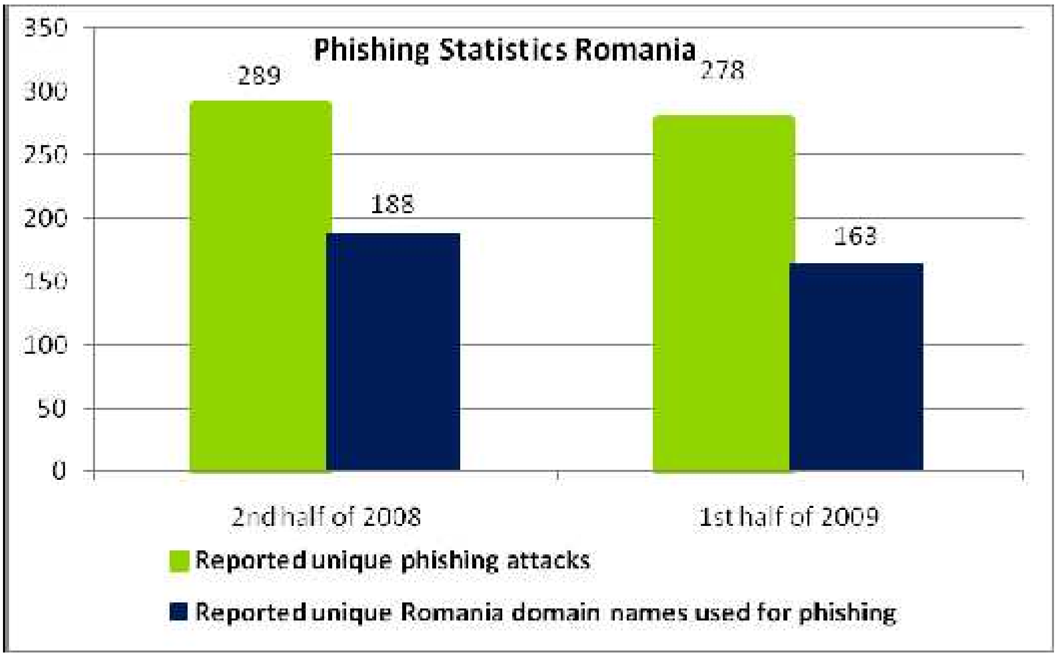
III.1. Security incident management

Local information security incidents are reported as public information on the web site of RoCSIRT[93]. This reporting is voluntary - users from within RoCSIRT constituency report mainly on the received phishing emails in which they are invited to disclose security related information. Local information security incidents reported in this manner cover phishing incidents related to the following Romanian banks:

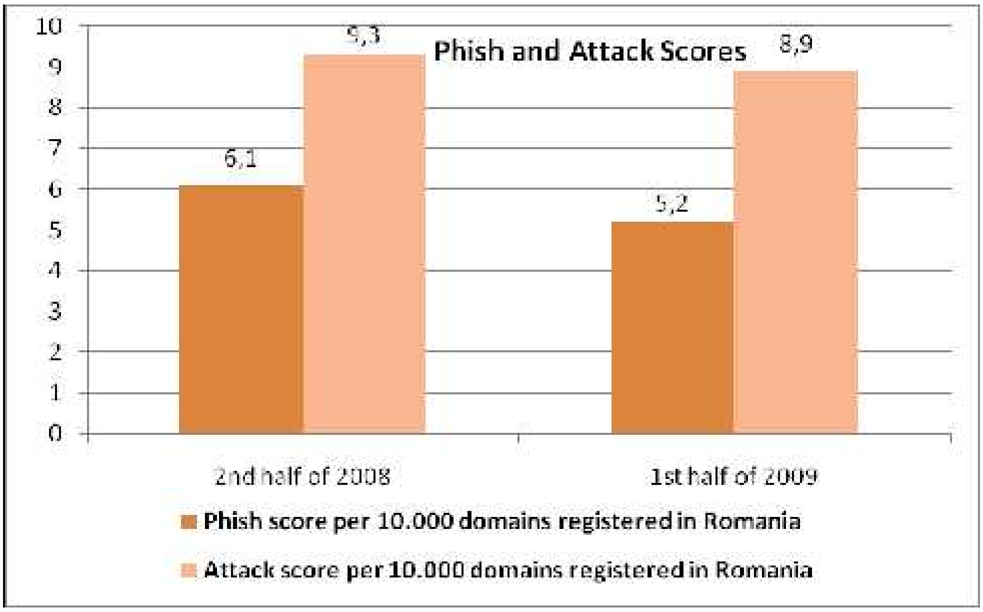
- BRD ;
- Bancpost ;
- Raiffeisen ;
- Transilvania;

Phishing incident information

It is interesting to mention that during the last half of 2008, and during the first half of 2009, Romania was reported in the global Top 20 Phishing TLDs in the report published by the Anti-Phishing Working Group (APWG)[94]:



[93] Computer Security Incident Response Team
[94] http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf



Other NIS-related incident reporting

The Ministry of Administration and Internal Affairs (MAI), and the Romanian Police have published in 2009 a report concerning the IT criminality and fraud, focused on incidents related to:

- Electronic commerce frauds;
- Credit card transactions frauds;
- Information security attacks;
- Child pornography .

No particular NIS incident reporting is either published by the Romanian Intelligence Service (SRI); the Foreign Intelligence Service (SIE); Ministry of Defence or by the Special Telecommunications Service (STS).

In general, providers in Romania do not voluntarily report security incidents. Such cases are usually reported by media, by NGOs and by consumer protection organizations.

III.2. Emerging NIS risks

Emerging NIS risks highlighted by the Ministry of Telecommunications and Information Society

A list of emerging NIS risks that are officially considered by the Ministry of Telecommunications and Information Society is included in the specific procedure (public document) concerning „The management of emergency situations related to the risks in the scope of the Ministry" – published in 2005[95].

[95] *See the procedure "Regulament Privind Managementul Situaţiilor de Urgenţă Specifice Tipurilor de Riscuri din Domeniul de Competenţă al Ministerului Comunicaţiilor şi Tehnologiei Informaţiei – 2005" available at: http://www.mcsi.ro/ . Note: the procedure is available in Romanian only.*

According to this document, the following emerging risks were considered at the level of Romanian NIS authorities:

- Risks of major eCommunications network disruptions and risks of major disruptions to IT systems, caused by incidents like: fire, nuclear accidents, earthquakes, explosions, natural disasters, cyber attacks;
- Risks of cyber attacks affecting the data flows of NIS stakeholders, leading to denial of services, data theft or fraud.

Emerging NIS risks highlighted by the Romanian Intelligence Service

A major objective of the Romanian Intelligence Service‘s activity is to prevent, through its antiterrorist unit, the threat from turning into a crime against national security, by disrupting all terrorist intentions or logistics and eliminating all vulnerabilities, risks or dangers – including NIS-related risks.

According to Romania‘s National Security Strategy, terrorism stands among the main threats to national security. Thus countering the risk factors triggered by the evolution of international terrorism and its influences on Romania‘s security has become a key security objective. The National Strategy for Preventing and Countering Terrorism (as approved by the Supreme Council of National Defence - CSAT) is the fundamental conceptual document on this topic.

III.3. Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented by the Romanian Law No. 677/2001 concerning the Processing of Personal Data and Free Circulation of Such Data.

The competent national regulatory authority on this matter is the Romanian National Supervisory Authority for Personal Data Processing[96] (ANSPDCP).

Personal Data and Sensitive Personal Data

The definition of personal data in the DPA(Data Protection Act) is closely based on the standard definition of personal data.

Under the Romanian DPA, sensitive personal data includes both:

(i) the standard types of sensitive personal data;

(ii) information about criminal offences or criminal proceedings.

Information Security aspects in the local implementation of the Data Protection Directive

Data controllers must comply with the general data security obligations.

Data protection breaches

[96] ANSPDCP - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

The DPA does not contain any obligation to inform the Supervisory Authority or data subjects of a security breach.

Enforcement

ANSPDCP is independent of any public authority or private entity and it receives notifications from personal data processors and complaints filed by people whose rights have been infringed. ANSPDCP has the power to control personal data processors and to apply administrative sanctions.

III.4. NIS awareness

In Romania, NIS awareness raising measures are undertaken by both competent authorities as well as by private companies, academic bodies and NGOs. Like in almost all EU Member States, Romania has several informative website and one or more complaint channel to present NIS awareness actions. Most of these websites are related to spam and/or malware, including advice on how to best protect against them.

Awareness measures to combat spam and/or malware

The Romanian Ministry of Communications and Information Society (MCIS) informs end users about spam and other internet related crimes via its website[97]. Also, in 2009, the national telecom regulator launched a website with information regarding online malpractices such as spam, spyware, and also to start two campaigns against spam.

More information about the spam phenomena and guidelines regarding the measures to be taken by an end user against unsolicited commercial communications, are provided by private associations through their websites. The Romanian Association for Technology and Internet provides the first Romanian black list of spammers through its website.

Awareness actions related to the Internet safety for children

We noted particular attention given by the involved Romanian NIS authorities towards the awareness aspects related to the Internet safety for children.

The Programme – Safer Internet RO AN-HL-HELP SIGUR.INFO[98] - was establishing a Romanian combined node consisting of a hotline, a helpline and awareness activities with the aim to provide teachers, parents and child protection specialists with knowledge and tools to protect their children in the new technological environment. The node is created by a consortium comprising two non-governmental organisations - Save the Children Romania as a National Coordinator, Focus Romania - Hotline Coordinator and the company Positive Media, with

[97] *See: http://www.mcsi.ro*

[98] *See: http://www.sigur.info*

expertise in areas directly connected to children‘s rights, child protection and current new information technologies.

Awareness measures towards cybercrime

The Service for Combating Cybercrime under the Romanian Directorate for Investigating Organised Crime and Terrorism Offences of the Prosecutor‘s Office of the High Court of Cassation and Justice (DIICOT) is promoting a series of permanent measures in order to fight against cybercrime, such as:

- actions to increase public awareness and education about the danger of the computer crimes;
- hotlines allowing citizens who discover online illegal activities to report the conduct to relevant authorities (in Romania: www.efrauda.ro);
- cooperation activities between all institutions (at national and international level) and law enforcement agencies in fighting against cybercrime;
- encourage the private sector (including Internet Service Providers) and civil society (including teachers, non-governmental organizations, the media) to report any information they might obtain concerning cybercrime to the appropriate law enforcement or social service authority;
- stimulate the Internet service providers to contribute by facilitating the referral of relevant information to law enforcement authorities;
- training for criminal justice professionals (law enforcement, prosecutors and the judges) is a necessary as a part of a comprehensive program designed to fight these crimes. Provide special training for judges, prosecutors and police officers.

Other awareness-raising events

An annual International Conference on Computers, Communications and Control (ICCC)[99] takes place annually in Romania. The publishing policy of ICCC is to encourage particularly the publishing of scientific papers that are focused on the convergence of the 3 „C”(Computing, Communications, Control).

The event is open to government, academic and industry bodies and provides a forum for international scientists to present and discuss their latest research findings on a broad array of topics in computer networking and control. Topics of interest include:

- Applications of the Information Systems;
- Artificial Intelligence;
- Cryptography and Security;

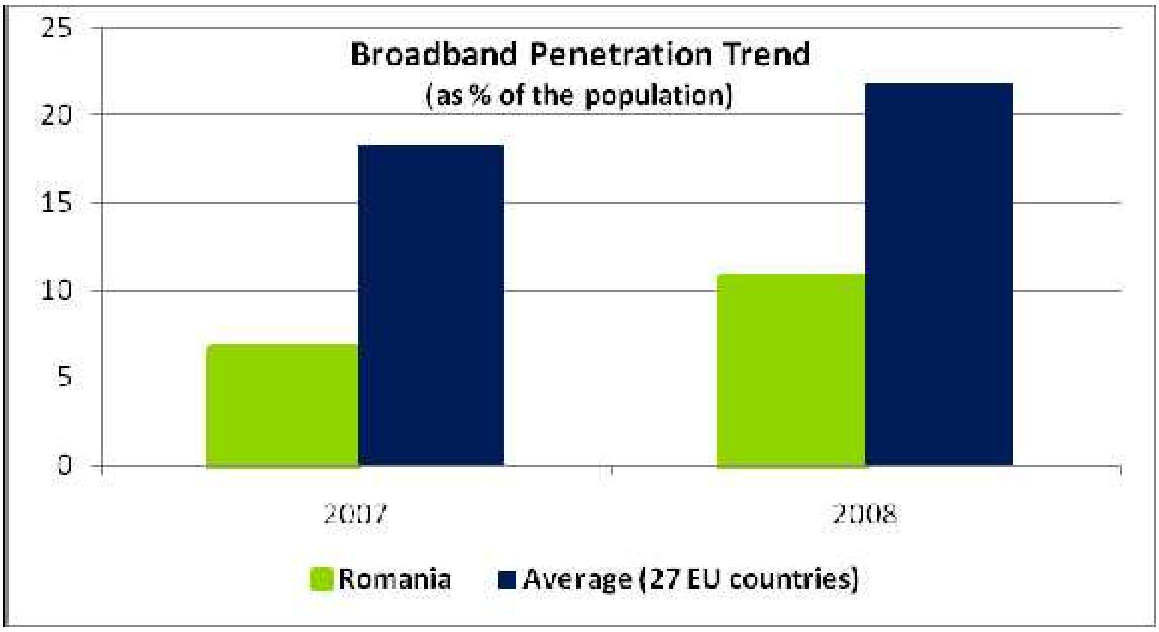
[99] *See* http://www.iccc.univagora.ro

- E-Activities;
- Fuzzy Systems;
- Informatics in Control;
- Information Society - Knowledge Society;
- Network Design & Internet Services;
- Multimedia & Communications

III. 5. Relevant statistics

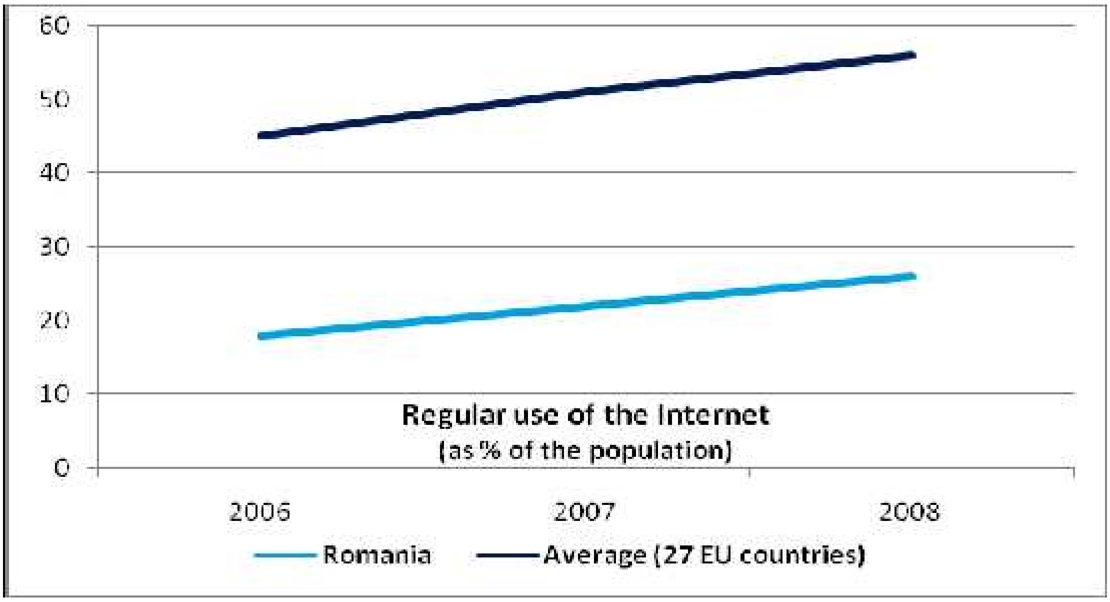
In order to provide an overview of recent IT developments in Romania, we present a few indicators in this section. The indicators show the current IT market development stage as they clearly have an impact on network and information security aspects.

Based on the Eurostat[100] information, it appears that the broadband penetration trend for Romania is significantly below the EU average:



Based on the same source of information, the regular use of Internet by the population (use as % of the population) is constantly below the EU average but it continues on an increasing path. Rates of Internet usage have been gradually improving over the last few years:

[100] *Source: Eurostat*



III. 6. Computer crimes covered by the Romanian Anti-corruption Law

Art.42	(1) The illegal access to a computer system- imprisonment from 6 months to 3 years. (2) If the fact mentioned at item (1) is performed by infringing the security measures, the punishment is imprisonment from 3 to 12 years.
Art.43	1) The illegal interception of any transmission of computer date that is not published to, from or within a computer system- imprisonment from 2 to 7 years. (2) The same punishment is applied also for the illegal interception, of electromagnetic emissions from a computer system carrying non-public computer data.
Art.44	(1) The illegal alteration, deletion or deterioration of computer data of the access restriction to such data- imprisonment from 2 to 7 years. (2) The unauthorised data transfer from a computer system- imprisonment from 3 to 12 years. (3) The unauthorised data transfer by means of an information data storing mean is also punish as in paragraph (2).
Art.45	The serious hindering, without right, of a computer system operation, by the introducing, transmitting, altering, deleting or deteriorating computer data or by restricting the access to these data- imprisonment from 3 to 15 years.

Art.46	(1) The following are considered criminal offences and punished with imprisonment from one to 6 years. a) the production, sale, import, distribution or making available, in any other form, without right, of a device or a computer programme designed or adapted for the purpose of committing one of the offences established in accordance with arts.42-45; b) the production, sale, import, distribution or making available, in any other form, without right, of a password, access code or other such computer data allowing total or partial access to a computer system for the purpose of one of the offences established in accordance with arts.42-45; (2) The possession, without right, of a device, computer programme, password, access code or computer data referred to at paragraph (1) for the purpose of one of the offences established in accordance with arts.42-45 is also punished similarly.

Apendix 1 **Romanian specific NIS glossary**

AARNIEC	Agenția de Administrare a Rețelei Naționale de Informatică pentru Educație şi Cercetare
ANCOM	Romanian National Authority for Communications
ANSPDCP	Romanian National Supervisory Authority for Personal Data Processing / Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
APWG	Anti-Phishing Working Group
ASSI	Agency for Information Society Services
Broadband Penetration Indicator	Number of total subscriptions to broadband connections (households, enterprises, public sector) by platform (DSL, all others) divided by the number of inhabitants. 3G subscriptions are not included in the total. Source: European Commission.
CERT	Computer Emergency Response Team (Centre de reacție şi răspuns la incidentele de securitate informatică)
CSIRT	Computer Security Incident Response Team
CSAT	Supreme Council of National Defence
DIICOT	Directorate for Investigating Organised Crime and Terrorism Offences of the Prosecutor‘s Office of the High Court of Cassation and Justice
DPA	Data Protection Act
EMIS	Romanian national Emergency Management Information System
GIS	Geographical Information Systems
ICCC	International Conference on Computers, Communications and Control
MCIS	Ministry of Communications and Information Society
MIRA	Ministry of Internal Affairs
NGO	Non-Governmental Organizations
NIS	network and information security
PBL	Phishing Black List
SBL	Spam Black List
SIE	Foreign Intelligence Service
SRI	Romanian Intelligence Service
STS	Special Telecommunications Service

CONCLUSIONS

Romania took important steps in development the eGovernment and eSociety. It has prepared all regulatory framework and key stakeholders. But, lack of Internet access and IT skills are the main barriers in Romania in the implementation of the NIS strategies and initiatives, but never the less the resistance to the Internet cannot be neglected as a large part of population seems to be not aware of its benefits.

Regarding the cyber attacks, the most widespread forms are the theft of identity and PIN card codes at either ATMs or upon online purchase payments. People have to inform ourselves about information security incidents and authorities must increase public awareness and education about the danger of the computer crimes.

REFERENCES

1. http://www.gov.ro/capitolul-14-societatea-informationala__l1a2077.html
2. http://www.mcsi.ro/Minister/Domenii-de-activitate-ale-MCSI/Comunicatii-electronice/Strategii
3. http://www.anrcti.ro
4. http://cert.org.ro/
5. http://www.cert-ro.eu
6. http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf
7. http://www.iccc.univagora.ro
8. http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/introduction
9. http://www.enisa.europa.eu
10. http://www.epractice.eu
11. http://www.roedu.net/
12. http://www.infosecurity-us.com/view/18274/federal-networks-attacked-15000-per-day-in-2010-says-dhs-official/
13. http://www.doingbusiness.ro/ro/stiri-afaceri/11862/romania-has-poor-management-of-information-security

DATA SECURITY ON SOCIAL NETWORKS

CAPT Andrei ZOTA

INTRODUCTION

Social networking sites are websites designed for human interaction. They enable users to meet others; keep in touch with them; and share experiences, feelings, and opinions. They are all built on a similar foundation—the user builds a network of contacts bound by an element of trust. The user then creates content for his/her friends and, in turn, accesses the content they have created. This content can include such diverse things as holiday pictures, interesting links, latest news, opinions, comments, and mood updates.

In both professional and personal life, human beings naturally form groups based on affinities and expertise. We gravitate to others with whom we share interests. Most of us belong to real world networks that formed organically. Not surprisingly, these networks rapidly migrated to the online world. Online social networking has been around in various forms for nearly a decade, and has begun to achieve wide notice in the past few years[101].

Online social networks take many forms, and are created for many reasons, like: to network with new contacts, reconnect with former friends, maintain current relationships, build or promote a business or project, participate in discussions about a certain topic, or just have fun meeting and interacting with other users.

Since their introduction, social network sites (SNSs) such as MySpace, Facebook, Cyworld, and Bebo have attracted millions of users, many of whom have integrated these sites into their daily practices. As of this writing, there are hundreds of SNSs, with various technological affordances, supporting a wide range of interests and practices. While their key technological features are fairly consistent, the cultures that emerge around SNSs are varied. Some sites cater to diverse audiences, while others attract people based on common language or shared racial, sexual, religious, or nationality-based identities. Sites also vary in the extent to which they incorporate new information and communication tools, such as mobile connectivity, blogging, and photo/video-sharing.

Social network tools have changed the way we interact in our personal lives and are in the process of transforming our professional lives. Increasingly, they play a significant role in how business gets done. But they're also high risk. With hundreds of millions of users, these tools have attracted attackers more than any other target in recent years.

[101] www.cerado.com

The information revolution has given birth to new economies structured around flows of data, information, and knowledge. In parallel, social networks have grown stronger as forms of organization of human activity[102].

That's why, the potential for mischief and malicious activities arises when one or more of those contacts breaks your trust. When that happens, a number of things can go wrong such as:

- Your contact's account was compromised and somebody else is using it.
- You added somebody to your network that you thought you knew but, in fact, you did not.
- You added somebody you thought was trustworthy but he/she turns out not to be.
- Insufficient use of privacy controls caused you to share data with people you never intended.

This document will cover the most common areas of attack using social networks and will recommend ways of minimizing risks. The goal of this paper is not to stop you from participating in social networks but to enable you to use them more safely.

II. PRIVACY IN A CONNECTED WORLD: DATA MINING IN SOCIAL NETWORKS

Social networks contain a wealth of personal information. People share their date of birth, email address, home address, family ties, and pictures. Some of that information would not be valuable by itself but having a clear picture of everything about a person can give attackers ideas and information required to perform other attacks such as credit card fraud or identity theft. Any real-life targeted attack can be made much more effective through access to additional information about the intended victim.

In addition to this, underground forums sell personal information. Your data can be mined and stored somewhere in the dark corners of the Internet waiting for a criminal to pay the right price for it. Criminals can use this information to obtain birth certificates/passports/other documentation and fake real-life identities. Some countries have looser controls than others, but in general, identity theft is something that already happens regularly.

Social networks contain a wealth of information. These include:

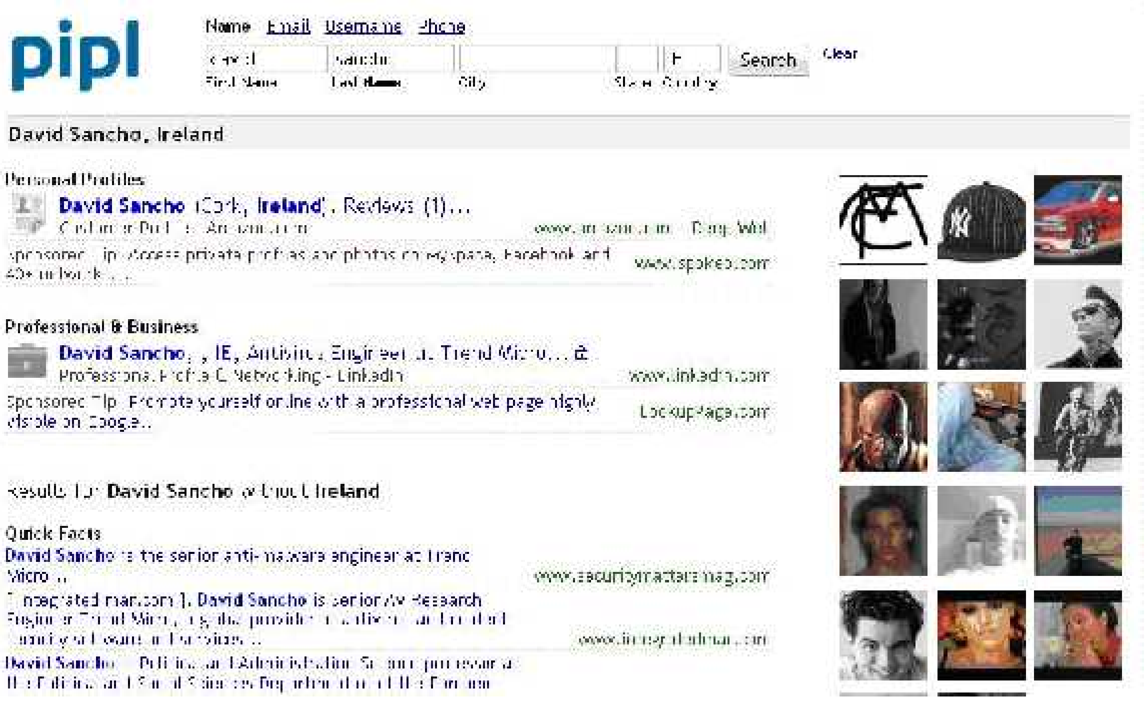
- Date of birth
- Email address
- Home address
- Family ties
- Pictures

[102] Social network analysis, Oliver Serrat

Other data that is of interest to criminals include email addresses, physical addresses, dates of birth, and affiliations:

- Email addresses are entered into databases that are later used for spam campaigns. Email addresses that come from social networks can be further categorized to improve the impact of the campaign—race, age, country and other factors can be used as filters in such a database so that its market price is higher than just any normal email address database. Email addresses can also be of great value in spear-phishing campaigns where they are often used as sender addresses. Spear-phishing is a very targeted phishing attack so using a known contact from a "friends" list adds credibility to the malicious email and increases the chances of success for the criminal.
- Real-life addresses are often shared in social networking sites and they too can be used to amass mailing databases for advertising purposes in a similar way as described above.
- Date of birth data is used by different companies to confirm people's identities over the telephone. Criminals do not have databases but they do have tools to automate "date of birth" searches in social networking sites. This proves that there is a demand for this information as a complementary piece in order to perpetrate certain types of fraud.

TrendLabs researchers have reported prices of personal information ranging from US$50 per stolen bank account credentials to about US$8 per million email addresses. This last figure is likely to be much higher if it involves fresh addresses coming from a social networking site.



David Sancho, Ireland

Personal Profiles

David Sancho (Cork, Ireland), Reviews (1)...
[illegible] www.[illegible].com

Sponsored Tip: Access private profiles and photos on MySpace, Facebook and 40+ networks... www.spokeo.com

Professional & Business

David Sancho, , IE, Antivirus Engineer at Trend Micro...
Professional Profile & Networking - LinkedIn www.linkedin.com

Sponsored Tip: Promote yourself online with a professional web page highly visible on Google.. LookupPage.com

Results for David Sancho in Cork Ireland

Quick Facts

David Sancho is the senior anti-malware engineer at Trend Micro ... www.securitymattersmag.com

[integrated mar.com]. David Sancho is senior AV Research Engineer at Trend Micro, [illegible] ... www.[illegible].com

David Sancho [illegible] Politics and Administration [illegible]

Figure 1. *Sample* PIPL *profile page*

Another factor that exacerbates this massive data-leakage potential is a user's public profile. When users set their information to be accessible without logging in to the social networking site, that information can be indexed in search engines or any other archive. There are social networking search engines that can search all available data about any name in a certain region. This makes the lives of stalkers, fraudsters, or any other attacker much easier. Not only do *Google* and other crawlers gather publicly available information but there are also meta-search engines like *pipl.com* specifically designed to search social networking sites and other sources to gather all sorts of information, from your name and the names of your friends to all the holiday pictures from three years ago that you already forgot you published online.

In July 2009, the wife of a high-level government executive in the United Kingdom published personal data in a social networking site. This garnered a lot of attention, not for the confidentiality of the content but for the lack of awareness there is about the accessibility of your online content. There is also another issue at play here, which is the fact that once you publish any picture online, you lose control over it as people leech and republish it on places you do not even know. In this case, news sites were some of the first to republish the infamous family pictures originally shared by the said executive's wife.

It is worth mentioning the fact that Human Resource (HR) departments are already utilizing information on social networks' public profiles to know more about job candidates. A certain online recruitment website reports that 20% of employers use social networking sites to run searches on job applicants and 68% use search engines like *Google* and *Yahoo!* to check on candidates. Although this common practice is not strictly illegal, it might be ethically questionable

SNS CONCEPT

A **network** is a set of nodes, points, or locations connected by means of data, voice, and video communications for the purpose of exchange.

Social refers to the interaction of people and other organisms with each other, and to their collective co-existence[103].

A **social network** is a description of the social structure between actors, mostly individuals or organizations. It indicates the ways in which they are connected through various social familiarities ranging from casual acquaintance to close familiar bonds.

In its simplest form, a social network is a map of specified ties, such as friendship, between the nodes being studied. The network can also be used to measure social capital – the value that an

[103] http://en.wikipedia.org/wiki/Social_(disambiguation)

individual gets from the social network. These concepts are often displayed in a social network diagram, where nodes are the points and ties are the lines[104].

We define **social network sites** [SNS] as web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site[105].

Social network analysis views social relationships in terms of network theory consisting of nodes and ties (also called edges, links, or connections). Nodes are the individual actors within the networks, and ties are the relationships between the actors. The resulting graph-based structures are often very complex. There can be many kinds of ties between the nodes. Research in a number of academic fields has shown that social networks operate on many levels, from families up to the level of nations, and play a critical role in determining the way problems are solved, organizations are run, and the degree to which individuals succeed in achieving their goals[106].

Examples of social networks include “Facebook”, “You Tube”, “Linkedin”, “Yahoo!Groups”, “Wikipedia”, “Myspace”, “Hi 5” and hundreds of other sites all focused on empowering individuals to:

a) connect with friends, colleagues or strangers;

b) create, contribute and publish content;

c) comment on, rank or embellish that content;

d) communicate freely and creatively using multiple formats including: email, instant messaging, mobile devices, voice and video and all for free or next to free in terms of real costs.

III. HISTORY OF SOCIAL NETWORK SITES

III.1. Timeline of social networks sites

Sporting a name based on the theory somehow associated with actor Kevin Bacon that no person is separated by more than six degrees from another, the site sprung up in 1997 and was one of the very first to allow its users to create profiles, invite friends, organize groups, and surf other user profiles. Its founders worked the six degrees angle hard by encouraging members to bring more people into the fold. Unfortunately, this "encouragement" ultimately became a bit too

[104] http://en.wikipedia.org/wiki/Social_network

[105] Social Network Sites: Definition, History, and Scholarship, Nicole Ellison

[106] http://en.wikipedia.org/wiki/Social_network

pushy for many, and the site slowly de-evolved into a loose association of computer users and numerous complaints of spam-filled membership drives. SixDegrees.com folded completely just after the turn of the millennium.

From 1997 to 2001, a number of community tools began supporting various combinations of profiles and publicly articulated Friends. AsianAvenue, BlackPlanet, and MiGente allowed users to create personal, professional, and dating profiles—users could identify Friends on their personal profiles without seeking approval for those connections. Likewise, shortly after its launch in 1999, LiveJournal listed one-directional connections on user pages. LiveJournal's creator suspects that he fashioned these Friends after instant messaging buddy lists—on LiveJournal, people mark others as Friends to follow their journals and manage privacy settings. The Korean virtual worlds site Cyworld was started in 1999 and added SNS features in 2001, independent of these other sites. Likewise, when the Swedish web community LunarStorm refashioned itself as an SNS in 2000, it contained Friends lists, guestbooks, and diary pages.

The next wave of SNSs began when Ryze.com was launched in 2001 to help people leverage their business networks. Ryze's founder reports that he first introduced the site to his friends—primarily members of the San Francisco business and technology community, including the entrepreneurs and investors behind many future SNSs. In particular, the people behind Ryze, Tribe.net, LinkedIn, and Friendster were tightly entwined personally and professionally. They believed that they could support each other without competing. In the end, Ryze never acquired mass popularity, Tribe.net grew to attract a passionate niche user base, LinkedIn became a powerful business service, and Friendster became the most significant, if only as "one of the biggest disappointments in Internet history"[107].

III.2. Most important social networks

In the following section we discuss about the SNSs that shaped the business, cultural, and research landscape.

Friendster—In 2003, Friendster hit the Internet and blew up. It quickly gained worldwide media attention and was featured in magazines such as Spin and Time.

Livejournal—Although Livejournal was created before Friendster, it started gaining popularity around the same time. Kids everywhere got to journal their lives and deepest emotions for everyone to see. But at this point, the whole social networking thing remained pretty much underground.

MySpace—Friendster and Livejournal didn't enjoy success for long. Enter MySpace. MySpace took Friendster's formula, combined it with the blogging of Livejournal, and quickly dominated

[107] Social Network Sites: Definition, History, and Scholarship, Nicole Ellison

the market. By 2007, MySpace was the undisputed champion. MySpace also became the go-to method for bands to get their music out to the masses. This tool became useful to small and big bands alike.

Facebook– Facebook started out as a social networking website for college kids. In fact, you had to enter the name of the college you attended to even sign up. So at the onset, MySpace was killing Facebook. However, FaceBook eventually decided to go public and make the site available to everyone, while adding new features. And by doing so, Facebook has successfully thrust social networking into the mainstream. Kids, adults, seniors, corporations—everyone has a Facebook account.

Twitter– Twitter started getting big around the time Facebook took over. And while Facebook is in the lead, Twitter fulfills a different niche. Twitter creators capitalized on the same notion as fast food providers. People want something quick and easy. So they limited "tweets" to a small word count and now it's one of the best ways to share news with the world. Athletes tweet from games. Reporters tweet breaking news before TV and newspapers can pick it up[108].

IV. SOCIAL NETWORK ANALYSIS

IV.1 Overview

Social network analysis [SNA] is the mapping and measuring of relationships and flows between people, groups, organizations, computers, URLs, and other connected information/knowledge entities. The nodes in the network are the people and groups while the links show relationships or flows between the nodes. SNA provides both a visual and a mathematical analysis of human relationships.

Social Network Analysis is an approach to analysing organizations focusing on a network-based view of the relationships between people and/or groups as the most important aspect. Going back to the 1950's, it is characterised by adopting mathematical techniques especially from graph theory. It has applications in organizational psychology, sociology and anthropology. Social Network Analysis provides an avenue for analysing and comparing formal and informal information flows in an organization, as well as comparing information flows with officially defined work processes.

The first goal of Social Network Analysis is to visualise relationships between people and/or groups by means of diagrams. The second goal is to study the factors which influence relationships (for example the age, cultural background, and previous training of the people involved) and also to study the correlations between relationships. The third goal is to draw out implications of the relational data, including bottlenecks where multiple information flows

[108] http://www.techvert.com/history-social-networking-sites

funnel through one person or section (slowing down work processes), situations where information flows does not match formal group structure, and individuals who carry out key roles that may not be formally recognised by the organization. The fourth and most important goal of Social Network Analysis is to make recommendations to improve communication and workflow in an organization[109].

IV.2 Social network analysis software

Social network analysis software is used to identify, represent, analyze, visualize, or simulate nodes (e.g. agents, organizations, or knowledge) and edges (relationships) from various types of input data (relational and non-relational), including mathematical models of social networks. The output data can be saved in external files. Various input and output file formats exist.

Network analysis tools allow researchers to investigate representations of networks of different size - from small (families, project teams) to very large (the Internet, disease transmission). The various tools provide mathematical and statistical routines that can be applied to the network model.

Visual representations of social networks are important to understand network data and convey the result of the analysis. Visualization is often used as an additional or standalone data analysis method.

Social network tools are:

- for business oriented social network tools: iPoint, NetMiner, InFlow, Keyhubs, Sentinel Visualizer, KXEN Social Network, NodeXL.;
- For large networks with millions of nodes: Sonamine or ORA;
- For mobile telecoms Idiro SNA Plus is recommended;
- An open source package with GUI for Linux, Windows and Mac, is Social Networks Visualizer or SocNetV, developed in Qt/C++;
- Another generic open source package for Windows, Linux and OS X with interfaces to Python and R is "igraph", "Tulip";
- Another generic open source package with [GUI] for Windows, Linux and OS X is RapidNet is a generic freely available open source solution for network analysis and interactive visual network exploration and drill-down;
- For Mac OS X a related package installer of SocNetV is available[110].

[109] Applying Social Network Analysis Concepts to Military C4ISR Architectures, Anthony Dekker

[110] http://en.wikipedia.org/wiki/Social_network_analysis_software

To understand networks and their participants, we evaluate the location of actors in the network. Measuring the network location is finding the centrality of a node. These measures give us insight into the various roles and groupings in a network -- who are the connectors, mavens, leaders, bridges, isolates, where are the clusters and who is in them, who is in the core of the network, and who is on the periphery?

V. CONSEQUENCES OF USING SOCIAL NETWORKS

V.1. Social network threats

When you share information online, you need to understand the potential risks, and you need to be wary of what you share and with whom. Attackers may use social networking services to spread malicious code, compromise users' computers, or access personal information about a user's identity, location, contact information, and personal or professional relationships. You may also unintentionally reveal information to unauthorized individuals by performing certain actions.

Social networking sites not only facilitate interacting with personal and professional contacts but also locating them in the first place. They are intended for both connecting and reconnecting people. It is fairly simple for miscreants to create a large network of contacts by using any number of underhanded techniques such as:

- Creating a fake celebrity profile and allowing people to add them to their contact lists.
- Creating a duplicate of somebody's profile and re-inviting all of their friends.
- Creating a profile, adding themselves to a medium-sized group or community, and inviting a number of members of the group (universities, schools, etc.). Then joining a second group and starting again.
- Creating a female profile and publishing a pretty picture of "herself" then letting people add him/her to their lists. A lot of people use social networking sites to meet their partners online and many of these sites have specific tools to facilitate this.

There are a number of strategies that allow an attacker to break the circle of trust and get into people's contact lists. A lot of social network users do not realize that their contact lists really is a circle of trust and by adding somebody they do not know—celebrities included—they are opening their data to untrusted parties.

Some sites do not have privacy controls in place, or the ones they have do not protect all user data. Even if they do have comprehensive privacy controls, the user is often not obligated to select who can access his/her data and is often dissuaded from using the available controls because they appear too complex or time-consuming. Many users simply do not bother to configure these controls, be it for laziness or lack of knowledge. This means that whether by the site's design or the user's lack of interest, personal data is needlessly exposed to strangers, search engines, and the wider online world.

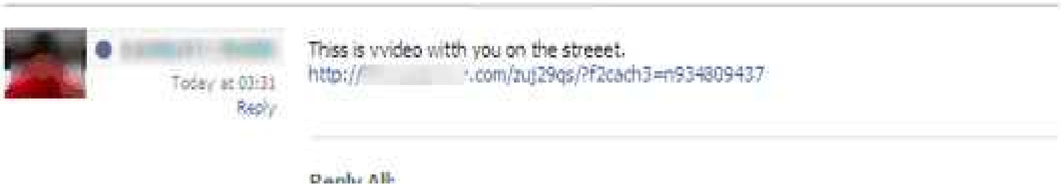
So, what can an attacker do with a large network of contacts in a social networking site?

One obvious possibility is advertise. The second possibility is collect contact information such as email addresses or telephone numbers. The third possibility is phishing and/ or malware installation.

Advertise. By writing/commenting on people's profiles or sending private mail, the attacker can distribute links advertising websites and products. If this strategy is done subtly, it can work relatively well, although usually this will be too much effort for any attacker. Contacts will quickly notice that the posts are covert advertising and will delete/block the attacker altogether. The same can be accomplished by private Web messaging, which all social sites allow but it is similarly ineffective for the same reasons stated above. These kinds of social networking spam runs are usually of a very limited duration and come from pay-per-click or pay-per-action affiliate-based online marketing schemes.

The second possibility is the **collection of contact information** such as email addresses or telephone numbers. Those social sites that display your friends' contact information can be used to amass working email databases along with phone numbers or other data that can serve to better target future spam, phishing, and vishing (voice phishing) campaigns. There are people amassing large contact databases, which are later sold to spammers, scammers, and credit card fraudsters. The value of such a database is measured on the quality of the data. Older email databases have been spammed over and over so the addresses might have been abandoned or accounts closed altogether. The more valuable email databases include fresh working emails such as the ones you can find in social networking sites. This kind of data is not only useful for conducting campaigns but also has value in itself and can be sold through the underground economy.

The third possibility is for **phishing and/or malware installation**. Imagine this scenario—the attacker creates a phishing page identical to *Facebook's* login page. Then they change their status line to "check this funny video I found yesterday" and a link to the fake page. When people click the link, they are presented with a fake *Facebook* login page, which they use to "log in" again, perhaps thinking that somehow their session had timed out. At this point, the attacker has the victim's username and password but the attack does not end there. After "logging in," the fake page displays a funny video that exploits a browser vulnerability and installs a Trojan in the background. This is not a hypothetical scenario but a high-level description of the activities of the malware known as "KOOBFACE" that have been successful spreading on a number of social networks. This is already happening and, as has always been the case with malware attacks, they will continue to get more and more complex as users become increasingly careful with the links they click.


[redacted]

Today at 03:31

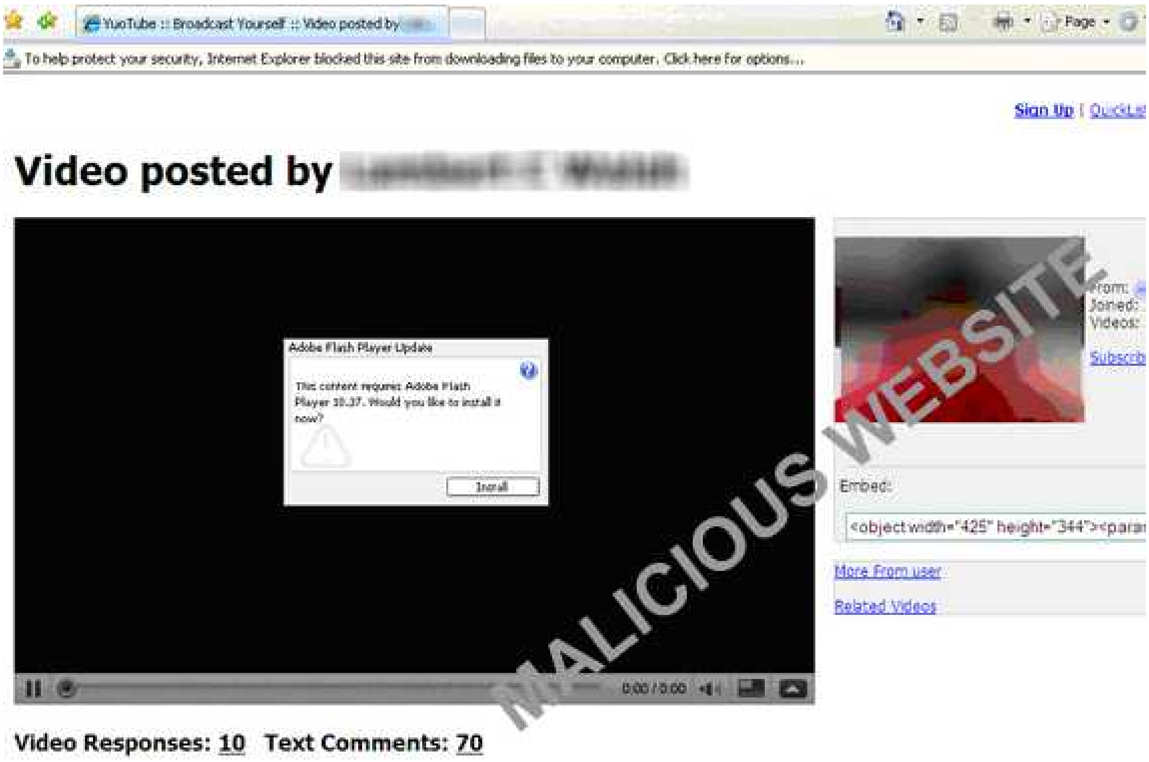
Reply

Thiss is vvideo witth you on the streeet.

http://[redacted].com/zuj29qs/?f2cach3=n934809437

Figure 2. *Sample malicious* Facebook *personal message*

This is the real danger of social and community-based sites—users trust their contacts to not send bad links, to not to try to infect their computers and take good care of their personal data. Once the trust is broken any of those situations can happen at any time.


YuoTube :: Broadcast Yourself :: Video posted by [redacted]

To help protect your security, Internet Explorer blocked this site from downloading files to your computer. Click here for options...

Video posted by [redacted]

Adobe Flash Player Update

This content requires Adobe Flash Player 10.37. Would you like to install it now?

Embed:

<object width="425" height="344"><param

Video Responses: 10 Text Comments: 70

Figure 3. *Sample malicious video linked to a* Facebook *personal message*

The real finesse comes from masking those bad links as if they were good. A normal user will probably have no problem clicking on a *youtube.com* link coming from an online contact but might be more careful with a *badsite.org* link. Enter URL shorteners. These online redirection services purposely hide a URL in order to make it shorter. Masked malicious URLs do not look dangerous before clicking on them. After that click, though, it is often too late. These shortening services are so widely used that people do not think twice before clicking one of them, even without knowing what lurks behind. URL shorteners are a security concern and should be taken very seriously.

Another attack vector is the exploitation of programming flaws in websites. These Web pages have been made by humans and they can have errors that could compromise the site's security measures. This has happened a number of times to well-known social networking sites and will likely happen again in the future. In these occurrences, all users are at risk. Poorly thought-out security, weak administration practices, or badly written code can all help an attacker to gather your data or help them stage a bigger attack against any number of users.

There have been instances of security flaws on *Facebook* that allowed anybody to access the "basic information" data of any user, no matter what their security settings were. This attack was released by casual users after *Facebook* ignored the users' warnings for a few days. No great knowledge was needed in this case to exploit a security weakness.

Twitter has had "cross-site scripting" attacks performed against it. In these cases, the attackers could change the *Twitter* status of any user accessing the attacker's account. This meant that the bad guys could make you tweet bad links so your *Twitter* followers would be at risk of being infected.

MySpace was attacked in 2007 by a JavaScript that would copy itself to the viewer's profile along with a piece of text—"Samy is my hero." This was caused by a security flaw that could have caused the victim to run any other command like redirecting the page to a malicious website. Thankfully, the young man who discovered the flaw and created the worm only wanted to have more friends added to his profile.

These three examples are not the only cases of security flaws on social networking sites. In fact, such flaws are identified frequently. News about such security holes are released every month and are a concern for all affected websites and their users. Since their solution is out of the user's hands, it is difficult or impossible to do anything about them.

Social networking sites keep adding to their security controls and refining their existing ones but, as in any development project, they also continue to innovate on their platforms and add exciting new features. These new options need to keep up with the security features or they too will suffer from security weaknesses. This is a cat-and-mouse game where the privacy and data security of the users are at stake.

V.2 Solutions

Social networking services are useful and enjoyable, but it is important to take proactive steps to protect your computer, your personal information, and your company data. By protecting yourself, you also help to protect the people you are connected to on these services.

Taking general security precautions will reduce the risk of compromise.

1. Use strong passwords, and use a unique password for each service.

2. Keep anti-virus software up to date.

3. Install software updates in a timely manner, particularly updates that affect web browsers.

Social networking services offer unique risks, and you can minimize these risks by adopting good security practices.

1. **Use strong privacy and security settings** – Take advantage of the security options provided by social networking services. When choosing appropriate options, err on the side of privacy to better protect your information. These services may change their options periodically, so regularly evaluate your security and privacy settings, looking for changes and ensuring that your selections are still appropriate. Also periodically review the services' privacy policies to see if there are any changes.
2. **Avoid suspicious third-party applications** – Choose third-party applications wisely. Look for applications developed by vendors you trust, and avoid applications that seem suspicious. Limit the amount of information third-party applications can access.
3. **Treat everything as public** – The best way to protect yourself is to limit the amount of personal information you post to these services. This recommendation applies not only to information in your user profile, but also to any comments or photos you post. It is important that you consider information that you post about yourself and about others, particularly children.
4. **Share only with people you know** – Although many users seek to establish as many contacts on these services as possible, consider sharing personal information only with people you know. If you expand your contacts beyond people you are sure you can trust, check the service's settings to see if you can group your contacts and assign different levels of access based on your comfort level. Attackers may adopt different identities to try to convince users to add them as contacts, so try to confirm that contacts are who they claim to be before giving them access to your information.

Regardless of how restrictive you make your security settings, they may not offer complete privacy. An attacker or application may take advantage of software vulnerabilities, or another user may repost your information. When using social networking services, be responsible and always consider the risks. Operate as if all of the content is public, and only post information you would be comfortable sharing with other people.

CONCLUSIONS

Social networking services are useful and enjoyable, but it is important to take proactive steps to protect your computer, your personal information, and your company data. By protecting yourself, you also help to protect the people you are connected to on these services.

Taking general security precautions will reduce the risk of compromise.

Social networking services offer both, unique and specific risks of any computer network and you can minimize these risks by adopting good security practices.

Social networking and community-based online services offer great fun and many benefits, both to individual users and to organizations. Users can reestablish contact with old school friends, find activity or even life partners, create art, and make new friends. Companies can leverage them to build their brand, get invaluable information about what their customers really think, and fix problems as they arise, among many other value-adding activities. However, social networking sites can also be a source of personal information leaks. They can also become a malware attack vector when not used cautiously.

There are ways to manage the risks. For starters, **you should only publish information that you are perfectly comfortable with, depending on what you want to accomplish.** In a dating site, you will want to state your age but not your exact birthday. Likewise, in a site where you plan to meet your high school friends, your year of graduation is probably the most important thing and date of birth will not be something you need to share at all. This may sound logical on a security standpoint but many people do not give it a second thought when opening their accounts.

The second recommendation is to **add only people you trust to your contact list.** Every time you receive a request from somebody to be your contact, ask yourself if you really trust that this person will keep your data safe and if their intentions are legitimate. If you are going to use the social network to meet new people and therefore plan to add unknown persons, set up a special email address and minimize the amount of personal information you share. In this case, **avoid clicking on unexpected links coming from them** and **never fully trust any of those contacts.**

REFERENCES

1. Social network analysis, Oliver Serrat
2. Social Network Sites: Definition, History, and Scholarship, Nicole Ellison
3. Applying Social Network Analysis Concepts to Military C4ISR Architectures, Anthony Dekker
4. www.cerado.com
5. http://en.wikipedia.org/wiki/Social_(disambiguation)
6. http://en.wikipedia.org/wiki/Social_network
7. http://en.wikipedia.org/wiki/Social_network
8. http://www.techvert.com/history-social-networking-sites
9. http://en.wikipedia.org/wiki/Social_network_analysis_software
10. http://www.orgnet.com/sna.html
11. http://www.us-cert.gov/reading_room/safe_social_networking.pdf
12. www.zdnet.co.uk/i/s/ads/.../WhitePaper_SocialNetworking.pdf
13. www.zdnet.co.uk/i/s/ads/.../WhitePaper_SocialNetworking.pdf
14. http://us.trendmicro.com/us/trendwatch/current-threat-activity/underground-economy/index.html
15. http://www.dailymail.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html
16. http://www.onrec.com/newsstories/17612.asp
17. http://www.scmagazineus.com/Facebook-bloggers-reveal-way-to-peek-at-private-profiles/article/138867/
18. http://blogs.computerworld.com/twitter_stalkdaily_mikeyy_xss_worm
19. http://www.betanews.com/article/CrossSite-Scripting-Worm-Hits-MySpace/1129232391

MySQL SERVER AND DATABASE SECURITY

LT Bogdan - George BERCIU

INTRODUCTION

MySQL is considered to be the most popular relational database management system in the world because it is free, it runs on a large variety of platforms, it's simple to use, easy to configure and performs very well even in significant load. Even if it is quite easy to configure there is a wide variety of security related configuration issues that makes securing it a real challenge.

MySQL represents a huge leap forward for the world's most popular database management system and while it has been the database of choice for managing high-volume sites and embedded database for years, the most recent versions provides exceptional new functionality that paves the way for larger adoption at the enterprise level.

I. GENERAL SECURITY ISSUES

When it comes to MySQL security we must think of a multitude of topics and how these might affect the security of our MySQL server and its related applications. As can be observed in the next graphic the level of vulnerabilities has grown among years.

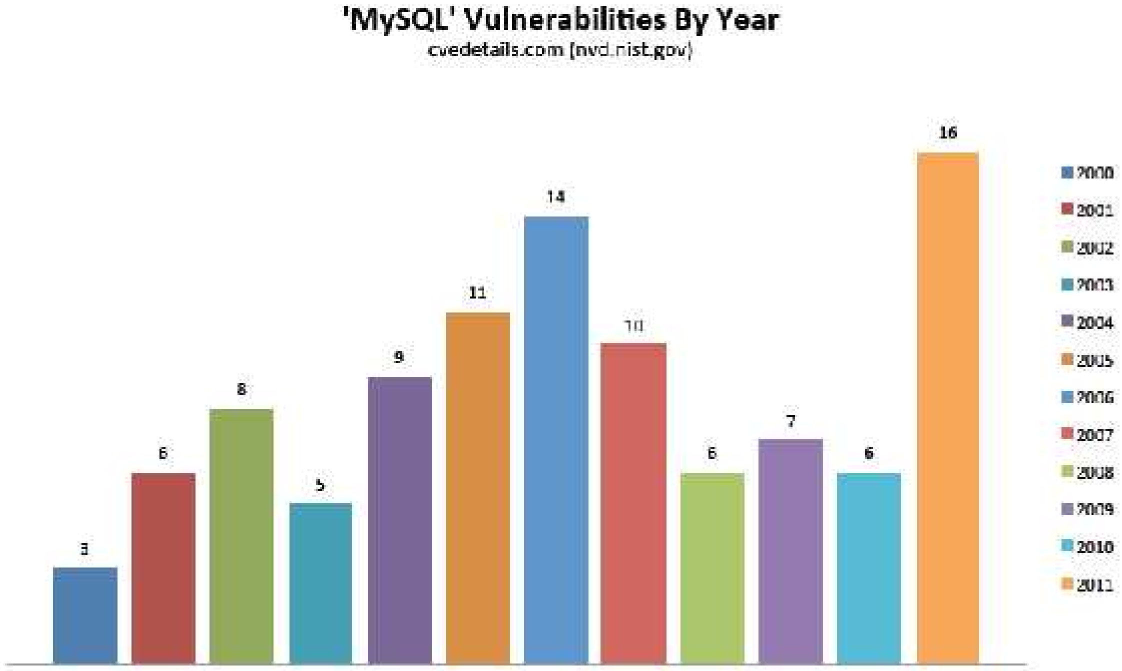


Figure 1

In the next lines I will talk about the following MySQL security related topics:

- The first topic is represented by the security of MySQL installation. There are many log files, data files, and application files of the installation that should be protected to ensure that they are not readable or writeable by unauthorized persons;
- The database security, including the users granted with access to the databases, views, stored procedures and access control ;
- The network security which is related to the grants for individual users;
- Security of applications to ensure that SQL attacks and other corruption of data does not occur;
- The necessity to perform the adequate backups of the database files, configuration and log files, and also to have a recovery solution in place and a test plan in order to successfully recover the information from the backups.

II. GUIDELINES FOR A SECURE MYSQL SERVER

When we speak about security, we emphasize the necessity of fully protecting the entire host, not just the MySQL server, against all types of possible attacks. Below are presented some examples:

- eavesdropping;
- altering;
- playback;
- denial of service (DoS).

MySQL uses security based on Access Control Lists (ACLs) for all connections, queries, and other operations that users can attempt to perform. There is also support for SSL-encrypted connections between MySQL clients and servers. Many of the concepts listed below are not specific to MySQL but these general ideas apply to almost all applications.

In the next lines I will present some guidelines to follow when running MySQL.

II.1. MySQL privileges

A critical measure is to not ever give anyone, except MySQL root accounts, access to the user table in the MySQL database. The GRANT and REVOKE statements are used for controlling access to MySQL. Do not grant more privileges than is necessary and never grant privileges to all hosts.

One way to check is to enter the following command:

```
mysql –u root
```

If the connection is successfully to the server without having to enter any password then anyone can connect to the MySQL server as the MySQL root user with full privileges.

Another way is to use the SHOW GRANTS statement to check which accounts have access to what. Then use the REVOKE statement to remove those privileges that are not necessary.

For example MySQL stores passwords for user accounts in the mysql.user table. Access to this table should never be granted to any non-administrative accounts. A user who has access to modify the plugin directory (the value of the "plugin_dir" system variable) or the "my.cnf" file that specifies the location of the plugin directory can replace plugins and modify the capabilities provided by plugins.

Passwords can appear as plain text in SQL statements such as CREATE USER, GRANT, and SET PASSWORD, or statements that invoke the "PASSWORD()" function. If these statements are logged by the MySQL server, the passwords become available to anyone with access to the logs. This applies to the general query log, the slow query log, and the binary log. To guard against unwarranted exposure to log files, they should be located in a directory that restricts access to only the server and the database administrator. If the administrator logs to tables in the mysql database, access to the tables should never be granted to any non- administrative accounts.

Replication slaves also store the password for the replication master in the "master.info" file. The access to this file should also be restricted to the database administrator. Also the database backups that include tables or log files containing passwords should be protected using a restricted access mode.

The access to some files can be also important when we speak about end-users because when a client program runs to connect to the MySQL server, it is inadvisable to specify the password in a way that exposes it to discovery by other users. In short, the safest methods are to have the client program prompt for the password or to specify the password in a properly protected option file.

II.2. Stored passwords

Do not store any plaintext passwords in the database. If the computer becomes compromised, the intruder can take the full list of passwords and use them. Instead is recommended to use MD5(), SHA1(), or some other one-way hashing function and store the hash value.

II.3. Password security

Do not choose weak passwords or passwords from dictionaries.

At the beginning of year 2010 Imperva, a company who offers database and application security for different organizations across the globe, has released a list of the 20 most commonly used, and therefore worst, passwords, culled from a hacking incident that took place in December 2009 at RockYou.com, a photo-sharing and slideshow site.

According to Imperva Application Defense Center (ADC) who analyzed the strength of passwords:

- About 30% of users chose passwords whose length is equal or below six characters ;

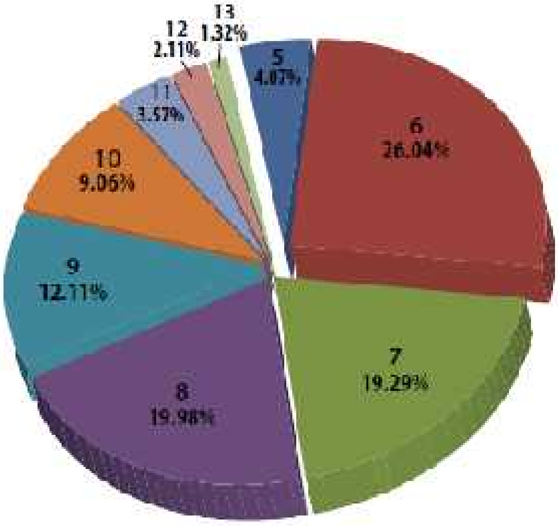


Figure 2 - Password length distribution

(according to Imperva Application Defense Center)

- Moreover, almost 60% of users chose their passwords from a limited set of alpha-numeric characters;

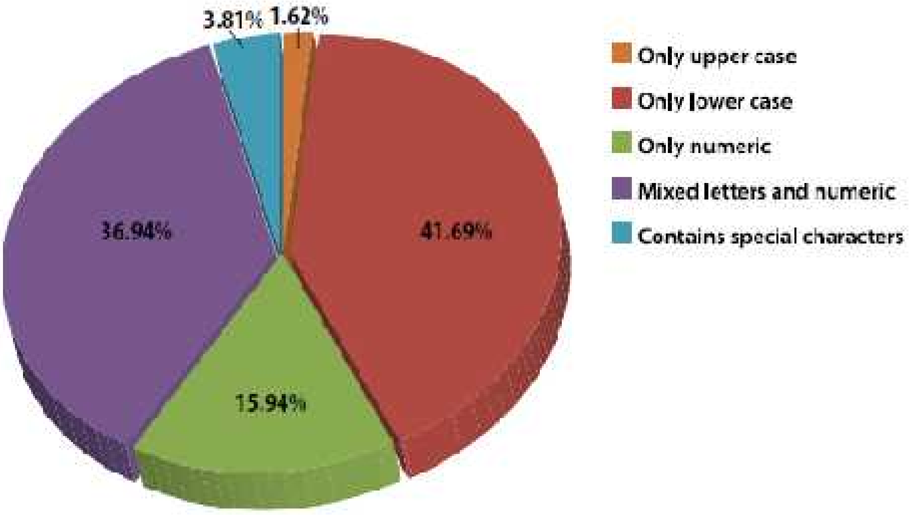
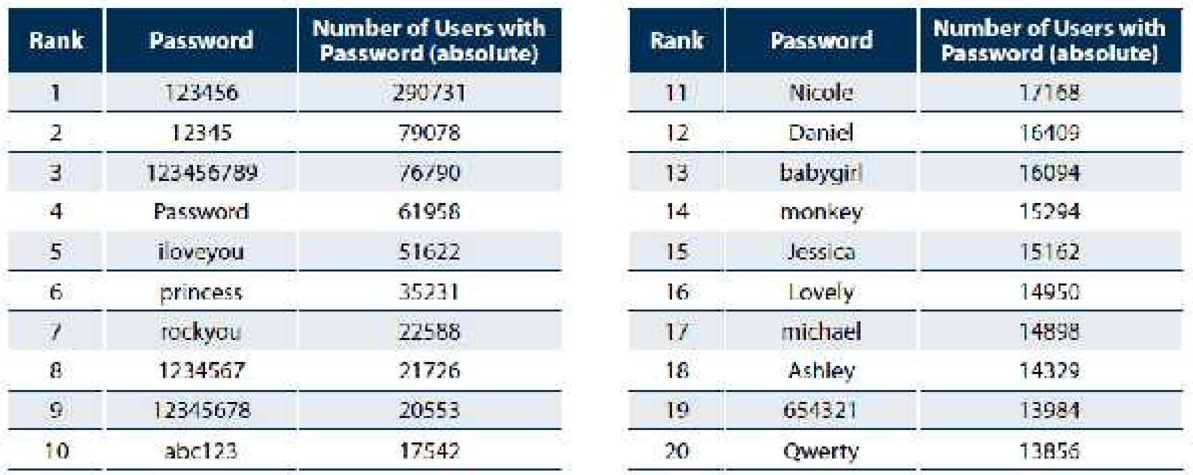


Figure 3 Password characters distribution

(according to Imperva Application Defense Center)

- Nearly 50% of users used names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys, and so on). The most common password among Rockyou.com account owners is “123456”.



Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

Figure 4 - Password popularity - Top 20

(according to Imperva Application Defense Center)

II.4. The Firewall protection

For a protection against at least 50% of all types of exploits in any software is recommended to use a firewall. MySQL server has to be behind a firewall or in a demilitarized zone (DMZ).

Nmap is a good tool for checking the ports that are open. MySQL uses port 3306 by default and this should be changed or secured in order not to be accessible from untrusted hosts. Another way is to check whether or not the 3306 port is open is to try the following command from some remote machine:

```
telnet [server_host] 3306
```

where, [server_host] is the host name or IP address of the host on which the MySQL server runs. If the connection is successfully and it returns some garbage characters, the port is open and should be closed on the firewall or router, unless it exist a good reason to keep it open. If telnet hangs or the connection is refused, the port is blocked, which is how it should be.

II.5. User data input

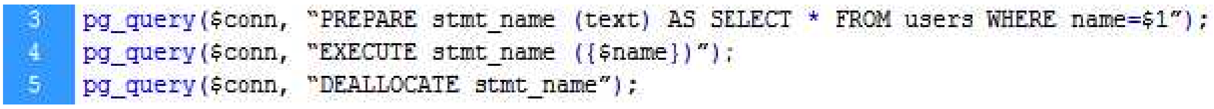
Do not trust any data entered by users in applications. They can try to trick the code by entering special or escaped character sequences in Web forms and URLs. The application must remain secure if a user enters something like “DROP DATABASE mysql”. This is an extreme example, but large security leaks and data loss might occur as a result of hackers using similar techniques. A common mistake is to protect only string data values, numeric data must be checked as well. If an application generates a query such as “SELECT * FROM table WHERE ID=234” when a user enters the value “234”, the user can enter the value “234 OR 1=1” to cause the application to generate the query “SELECT * FROM table WHERE ID=234 OR 1=1”. As a result, the server retrieves every row in the table. This exposes every row and causes excessive server load. The simplest way to protect from this type of attack is to use single quotation marks around the numeric constants like “SELECT * FROM table WHERE ID='234'”. If the user enters extra information, it all becomes part of the string. In a numeric context, MySQL automatically converts this string to a number and strips any trailing nonnumeric characters from it. Sometimes people think that if a database contains only publicly available data, it need not be protected. This is incorrect. Even if it is permissible to display any row in the database, the site should still be protected against denial of service attacks. Otherwise, the server becomes unresponsive to legitimate users.

The attack presented above is called SQL injection which is a common vulnerability that is the result of lax input validation. Unlike cross-site scripting vulnerabilities that are ultimately directed at the site’s visitors, SQL injection is an attack on the site itself, in particular its database. The goal of SQL injection is to insert arbitrary data, most often a database query, into a string that’s eventually executed by the database. The insidious query may attempt any number of actions, from retrieving alternate data, to modifying or removing information from the database. Fortunately many application programming interfaces provide a means of escaping special characters in data values. Properly used, this prevents application users from entering values that cause the application to generate statements that have a different effect than the one intended. Below are presented some methods used against SQL injection:

- MySQL C API: Use the “mysql_real_escape_string()” API call;
- Perl DBI: Use placeholders or the “quote()” method.

For example PHP has an automatic input escape mechanism, “magic_quotes_gpc”, which provides some rudimentary protection. If enabled, “magic_quotes_gpc”, or “magic quotes”, adds a backslash in front of single-quotes, double-quotes, and other characters that could be used to break out of a value identifier. But, “magic quotes” is a generic solution that doesn’t include all of the characters that require escaping, and the feature isn’t always enabled. Ultimately, it’s up to the developer to implement safeguards to protect against SQL injection.

Another way to prevent SQL injection is to use “Prepared queries” also known as “Prepared statements”. Prepared queries are query “templates”, this means that the structure of the query is pre-defined and fixed and includes placeholders that stand-in for real data. The placeholders are typically type-specific, for example, “int” for integer data and “text” for strings, which allows the database to interpret the data strictly. For instance, a text placeholder is always interpreted as a literal, avoiding exploits such as the query stacking SQL injection. A mismatch between a placeholder's type and its incoming data cause, execution errors, adding further validation to the query. In addition to enhancing query safety, prepared queries improve performance. Each prepared query is parsed and compiled once, but can be re-used over and over. If it's necessary to perform a long list of INSERT operations, a pre-compiled query can save valuable execution time. Preparing such a query is quite simple, below is presented a short PHP example:



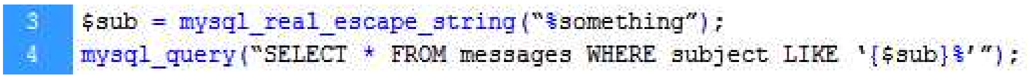
```
pg_query($conn, "PREPARE stmt_name (text) AS SELECT * FROM users WHERE name=$1");
pg_query($conn, "EXECUTE stmt_name ({$name})");
pg_query($conn, "DEALLOCATE stmt_name");
```

Figure 5 – Using prepared statements

As nice as prepared queries are, not all databases support them; fortunately this feature is available in MySQL starting with version 4.1.

The SQL "LIKE" operator is another extremely valuable feature, its % and _ (underscore) qualifiers match 0 or more characters and any single character, respectively, allowing for flexible partial and substring matches. However, both LIKE qualifiers are ignored by the database's own escape functions and PHP's magic quotes. Consequently, user input incorporated into a LIKE query parameter can subvert the query, complicate the LIKE match, and in many cases, prevent the use of indices, which slows a query substantially. With a few iterations, a compromised LIKE query could launch a Denial of Service attack by overloading the database.

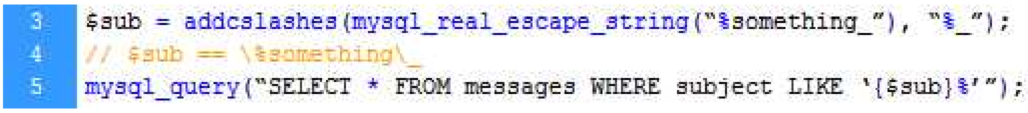
Here's a simple yet effective attack:



```
$sub = mysql_real_escape_string("%something");
mysql_query("SELECT * FROM messages WHERE subject LIKE '{$sub}%'");
```

Figure 6 – A simple attack example using the LIKE operator

The intent of the SELECT above is to find those messages that begin with the user-specified string, $sub. Uncompromised, that SELECT query would be quite fast, because the index for subject facilitates the search. But if $sub is altered to include a leading % qualifier, the query can't use the index and the query takes far longer to execute, the query gets progressively slower as the amount of data in the table grows. The underscore qualifier presents similar problems. A method to specify a character range to an escape is to use "addcslashes()".

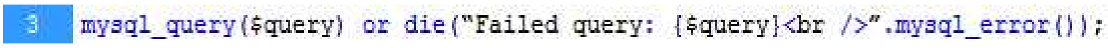


```
$sub = addcslashes(mysql_real_escape_string("%something_"), "%_");
// $sub == \%something\_
mysql_query("SELECT * FROM messages WHERE subject LIKE '{$sub}%'");
```

Figure 7 - Using the "addcslashes()" function

Here, the input is processed by the database's prescribed escape function and is then filtered through addcslashes() to escape all occurrences of % and _. addcslashes() works like a custom addslashes(), is fairly efficient, and much faster alternative that str_replace() or the equivalent regular expression. Applying manual filters after the SQL filters to avoid escaping the backslashes is always a good practice; otherwise, the escapes are escaped, rendering the backslashes as literals and causing special characters to re-acquire special meanings.

Another issue regarding database security is related to MySQL error handling. One common way for hackers to spot code vulnerable to SQL injection is by using the developer's own tools against them. For example, to simplify debugging of failed SQL queries, many developers echo the failed query and the database error to the screen and terminate the script.



```
mysql_query($query) or die("Failed query: {$query}<br />".mysql_error());
```

Figure 8 – Displaying a failed query

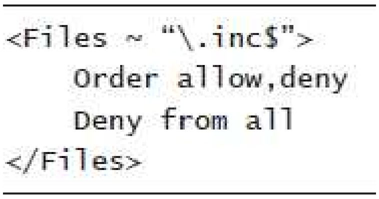
While very convenient for spotting errors, this code can cause several problems when deployed in a production environment. The above code may reveal a great deal of information about the application or the site. For instance, the end-user may be able discern the structure of the table and some of its fields and may be able to map GET/POST parameters to data to determine how to attempt a better SQL injection attack. In fact, the SQL error may have been caused by an inadvertent SQL injection. Hence, the generated error becomes a literal guideline to devising more tricky queries.

The best way to avoid revealing too much information is to devise a very simple SQL error handler to handle SQL failures. This error handler could take the query and the error message generated by the database and create an error string based on that information. The error string should be passed through htmlspecialchars() to ensure that none of the characters in the string are rendered as HTML, and the string should append to a log file.

The next step depends on whether or not the script is working in debug mode or not. If in debug mode, the error message is returned and is likely displayed on-screen for the developer to read. In production, though, the specific message is replaced with a generic message, which hides the root cause of the problem from the visitor.

Perhaps the final issue to consider when working with databases is how to store the application's database credentials, the login and password that grant access to the database. Most applications use a small PHP configuration script to assign a login name and password to variables. This configuration file, more often than not, is left unprotected and readable to provide the web server user access to the file. But readable means just that, anyone on the same system or an exploited script can read the file and steal the authentication information stored within. Worse, many applications place the configurations file inside web readable directories and give it a non-PHP extension like ".inc" which is the most popular choice. Since ".inc" is typically not configured to be interpreted as a PHP script, the web browser displays such a file as plain-text for all to see.

One solution to this problem uses the web server’s own facilities, such as .htaccess in Apache, to deny access to certain files. As an example, this directive denies access to all files that end with the string “.inc”



```
<Files ~ “\.inc$”>
    Order allow,deny
    Deny from all
</Files>
```

.

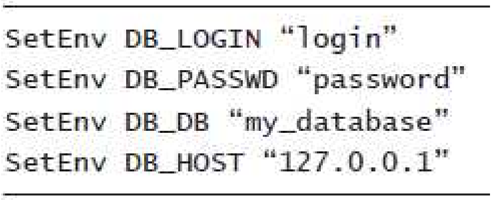
Figure 9 – Editing .htaccess file to block all files that end with the string “.inc”

Alternatively, PHP can be configured to treat “.inc” files as scripts or simply changing the extension of the configuration files to “.php” or “.inc.php” which denotes that the file is an include file. However, renaming files may not always be the safest option, especially if the configuration files have some code aside from variable initialization in the main scope. The ideal and simplest solution is to simply not keep configuration and non-script files inside web server-accessible directories but that still leaves world-readable files vulnerable to exploit by local users.

One seemingly effective solution is to encrypt the sensitive data. Database authentication credentials could be stored in encrypted form, and only the applications that know the secret key can decode them. But this use of encryption only makes theft slightly more difficult and merely shifts the problem instead of eliminating it. The secret key necessary to decrypt the credentials must still be accessible by PHP scripts running under the web server user, meaning that the key must remain world-readable.

A proper solution must ensure that other users on the system have no way of seeing authentication data. Fortunately, the Apache web server provides just such a mechanism. The Apache configuration file, “httpd.conf” can include arbitrary intermediate configuration files during start-up while Apache is still running as root. Since root can read any file, the sensitive information can be placed in a file in home directory and changed to mode 0600, so only the creator and the superuser can read and write the file.

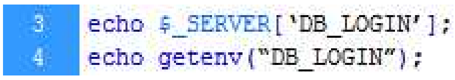
The content of the configuration file is a series of “SetEnv” lines, defining all of the authentication parameters necessary to establish a database connection.



```
SetEnv DB_LOGIN “login”
SetEnv DB_PASSWD “password”
SetEnv DB_DB “my_database”
SetEnv DB_HOST “127.0.0.1”
```

Figure 10 – Authentication parameters from httpd.conf file

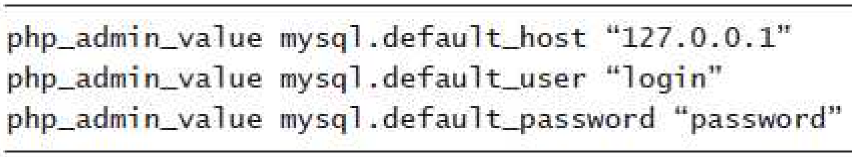
After Apache starts, these environment variables will be accessible to the PHP script via the $_SERVER super-global or the getenv() function if $_SERVER is unavailable.



```
echo $_SERVER['DB_LOGIN'];
echo getenv("DB_LOGIN");
```

Figure 11 – Accessing the environment variables

An even better method of this trick is to hide the connection parameters altogether, hiding them even from the script that needs them like using PHP's ini directives to specify the default authentication information for the database extension. These directives can also be set inside the hidden Apache configuration file.



```
php_admin_value mysql.default_host "127.0.0.1"
php_admin_value mysql.default_user "login"
php_admin_value mysql.default_password "password"
```

Figure 12 – Authentication parameters using PHP's ini directives

Now, mysql_connect() works without any arguments, as the missing values are taken from PHP ini settings. The only information remaining exposed would be the name of the database. Because the application is not aware of the database settings, it consequently cannot disclose them through a bug or a backdoor, unless code injection is possible. In fact, can be enforced the fact that only an ini-based authentication procedure can be used by enabling SQL safe mode in PHP via the sql.safe_mode directive. PHP then will reject any database connection attempts that use anything other than ini values for specifying authentication data.

II.6. Secured connection

Do not transmit plain (unencrypted) data over the Internet. This information is accessible to everyone who has the time and ability to intercept it and use it for their own purposes. Instead, use an encrypted protocol such as SSL or SSH. MySQL supports internal SSL connections as of version 4.0. Another technique is to use SSH port-forwarding to create an encrypted (and compressed) tunnel for the communication.

Nowadays is used everywhere in a large variety of applications like:

- Browsers;
- Email;
- Routers;
- Factory Automation;
- VoIP;
- Automobile Communications;
- Sensors;

- Smart Power Meters and much more.

By default, MySQL uses unencrypted connections between the client and the server.

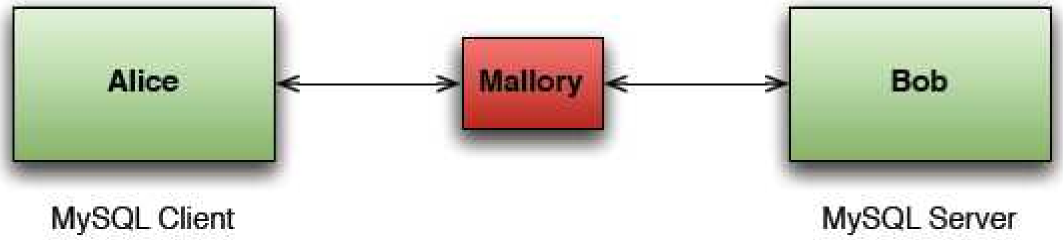


Figure 13 – The communication between the MySQL client and server

Data flowing between a client and a MySQL server is not unlike any other typical network traffic; it could potentially be intercepted and even modified by a malicious third party. Sometimes this isn't really an issue because the database server and clients often reside on the same internal network and, for many, on the same machine. However, if the application requirements result in the transfer of data over insecure channels, there is the option to use MySQL's built-in security features to encrypt that connection.

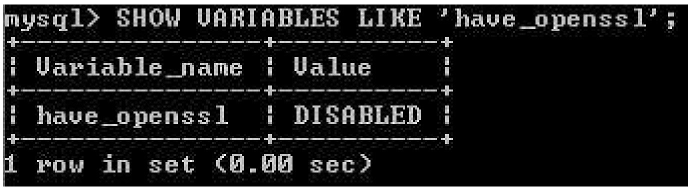
As of version 4.0.0, it became possible to encrypt all traffic between the MySQL client and server using SSL and the X509 encryption standard. To implement this feature, there are a few steps to follow first, unless there is running MySQL 5.0.10 or greater, in which case these versions come bundled with yaSSL support, meaning OpenSSL is no longer needed to implement secure MySQL connections.

However if MySQL 5.1.11 or earlier is running at the configuration time MySQL need to know whether yaSSL will be used by including the "--with-ssl" option, or OpenSSL by including the "--with-ssl=/path/to/openssl" option.

Regardless of whether is used yaSSL or require OpenSSL, all of the other instructions are identical.

- Install the OpenSSL library, available for download at www.openssl.org.
- Configure MySQL with the "--with-vio" and "--with-openssl" flags.

Whether MySQL is ready to handle secure connections can be verified by logging in to the MySQL server and executing the following command:



```
mysql> SHOW VARIABLES LIKE 'have_openssl';
+---------------+----------+
| Variable_name | Value    |
+---------------+----------+
| have_openssl  | DISABLED |
+---------------+----------+
1 row in set (0.00 sec)
```

Figure 14 – Verifying if MySQL is ready to handle secure connections

As the picture above shows, the “have_openssl” variable is disabled. Once the steps to enable this option are complete, the administrator must create or purchase both a server certificate and a client certificate.

II.7. The database backup

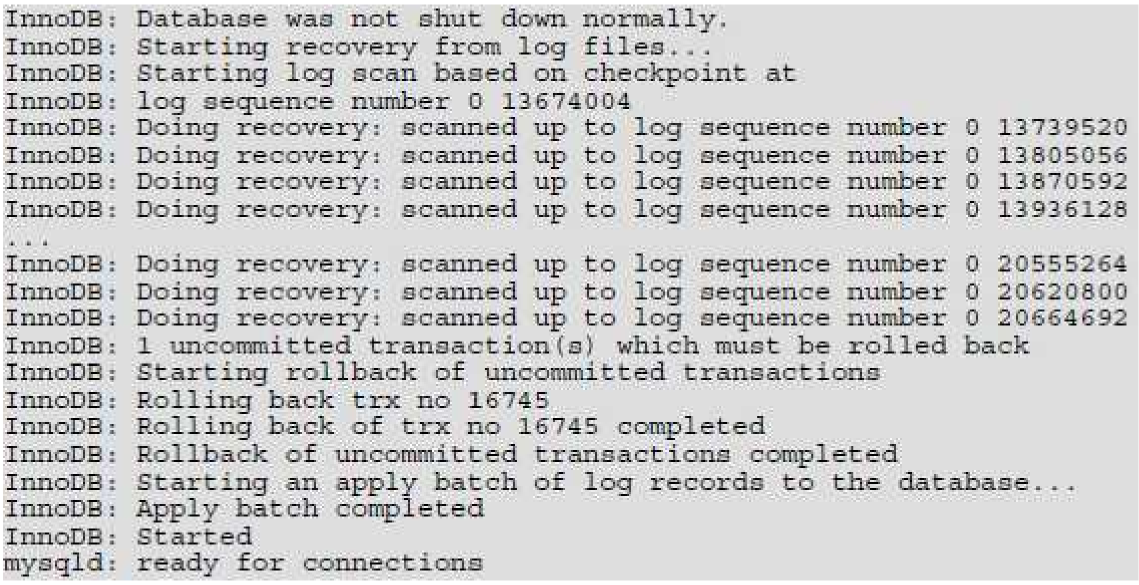
Performing the adequate backups of the database files, configuration and log files, and also having a recovery solution in place and a test plan in order to successfully recover the information from the backups is another important issue to consider when we speak about database security.

There are a lot of moments when is important to have a backup solution like:

- Operating system crash;
- Power failure;
- File system crash;
- Hardware problem (hard drive, motherboard, and so forth).

The example commands do not include options such as “–user” and “—password” for the “mysqldump” and “mysql” programs. The administrator should include such options as necessary so that the MySQL server allows him to connect to it.

Let’s assume that data is stored in the InnoDB storage engine, which has support for transactions and automatic crash recovery. We also assume that the MySQL server is under load at the time of the crash. If it were not, no recovery would ever be needed. For cases of operating system crashes or power failures, we can assume that MySQL's disk data is available after a restart. The InnoDB data files might not contain consistent data due to the crash, but InnoDB reads its logs and finds in them the list of pending committed and non-committed transactions that have not been flushed to the data files. InnoDB automatically rolls back those transactions that were not committed, and flushes to its data files those that were committed. Information about this recovery process is conveyed to the user through the MySQL error log.



```
InnoDB: Database was not shut down normally.
InnoDB: Starting recovery from log files...
InnoDB: Starting log scan based on checkpoint at
InnoDB: log sequence number 0 13674004
InnoDB: Doing recovery: scanned up to log sequence number 0 13739520
InnoDB: Doing recovery: scanned up to log sequence number 0 13805056
InnoDB: Doing recovery: scanned up to log sequence number 0 13870592
InnoDB: Doing recovery: scanned up to log sequence number 0 13936128
...
InnoDB: Doing recovery: scanned up to log sequence number 0 20555264
InnoDB: Doing recovery: scanned up to log sequence number 0 20620800
InnoDB: Doing recovery: scanned up to log sequence number 0 20664692
InnoDB: 1 uncommitted transaction(s) which must be rolled back
InnoDB: Starting rollback of uncommitted transactions
InnoDB: Rolling back trx no 16745
InnoDB: Rolling back of trx no 16745 completed
InnoDB: Rollback of uncommitted transactions completed
InnoDB: Starting an apply batch of log records to the database...
InnoDB: Apply batch completed
InnoDB: Started
mysqld: ready for connections
```

Figure 15 – An example log excerpt

For the cases of file system crashes or hardware problems, we can assume that the MySQL disk data is not available after a restart. This means that MySQL fails to start successfully because some blocks of disk data are no longer readable. In this case, it is necessary to reformat the disk, install a new one, or otherwise correct the underlying problem. Then it is necessary to recover our MySQL data from backups, which means that we must already have made backups. To make sure that is the case, it should exist a designed backup policy.

II.8. The Backup policy

The backups must be scheduled periodically. A full backup of the database represents a snapshot of the data at a point in time and it can be done in MySQL with several tools. For example, InnoDB Hot Backup provides online non-blocking physical backup of the InnoDB data files, and mysqldump provides online logical backups.

Full backups are necessary, but they are not always convenient. They produce large backup files and take time to generate. They are not optimal in the sense that each successive full backup includes all data, even that part that has not changed since the previous full backup. After the initial full backup is made, it is more efficient to create incremental backups. They are smaller and take less time to produce. The trade-off is that, at recovery time, the data cannot be restored just by reloading the full backup. The administrator must also process the incremental backups to recover the incremental changes.

II.9. The MySQL logs

Verifying the MySQL logs can also represent a source to identify a possible attack or a server error. MySQL has several different logs that can help the administrator to find out what is going on inside. Below are presented the MySQL logs and the information that is written in it:

- The error log contains problems encountered starting, running, or stopping MySQL;
- The general query log contains the established client connections and statements received from clients;
- The binary log contains all statements that change data;
- The slow query log contains all queries.

.

III. STEPS IN SECURING A MYSQL SERVER ON WINDOWS

With a few simple steps MySQL on Windows can be secured to prevent malicious users from accessing MySQL and the data it contains. As I presented above the key steps are to secure the default user accounts, limit external access, and use strong passwords. Those looking to increase the security of their server can run MySQL as a limited user, change the name of the root account, and even encrypt the MySQL data directory.

Step 1: Install MySQL on a recent, version of Windows and ensure that the host operating system is completely up to date with the latest service packs and patches.

Step 2: Install MySQL on an NTFS File System because this type of file system supports access controls, large files, and data encryption.

Step 3: Install MySQL on a Standalone Machine. In production, MySQL should be installed on a server machine dedicated to hosting the MySQL server. All services that are not required should be disabled and no extra applications should be run. This not only increases the stability of the server, it frees more system resources for MySQL and prevents third-party applications from being potential security threats. There should be no user logins allowed other than administrators.

Step 4: Install the Latest Production Version of MySQL. It is recommended that all users to upgrade to the latest stable version of MySQL. While security bug fixes are usually ported to previous versions of MySQL, using the latest production version ensures that the MySQL installation is as stable and secure as possible. Using pre-production software such as is not recommended for production servers as not all bugs have necessarily been identified and corrected, resulting in decreased stability and possibly decreased security.

Step 5: Secure the MySQL User Accounts. During the installation process, provide a root password when prompted. Ensure that your root password is a strong password, containing letters, numbers, and symbols. The password should be at least 6 characters long, should not contain any words found in a dictionary, and letters should be in mixed case.

In addition, the administrator can check the box marked “Root May Only Connect from Localhost” and leave the box marked “Create an Anonymous Account” unchecked. This will greatly increase the security of the MySQL installation.

Step 6: Disable TCP/IP Access. By default the MySQL server will allow connections via TCP/IP from any host but it can reject a connection based on the user's remote hostname or IP address. In many cases TCP/IP connectivity is not required and can be disabled to prevent remote access to the MySQL server. If MySQL is used locally for development or for use with a web server, the TCP/IP networking can be disabled.

Step 7: Bind the TCP/IP Address. In some situations the TCP/IP access cannot be disabled even when the server will only be needed for requests from “localhost”. In such situations can be added the following to the “[mysqld] “section of the server configuration file:

```
bind-address=127.0.0.1
```

This will cause the MySQL server to respond only to requests from localhost, and ignore all requests from the machine's network interfaces.

Step 8: Firewall the Server. As is presented above all server machines should be protected by a firewall as the first line of defense against a malicious user. Under no circumstances should the MySQL server be accessible to the Internet. When a MySQL server is used by client machines across a LAN it may be necessary a permit rule for external access to MySQL from other machines on the local network, but the LAN should be separated from the Internet by a firewall that blocks traffic on port 3306. At the very least a software firewall should be installed on the MySQL server that only permits connections from the local network and other trusted IP addresses. Ideally the administrator should place a hardware firewall between the MySQL server and the Internet. This does not mean users cannot access MySQL remotely, it is possible to use SSH port forwarding to tunnel MySQL traffic through a firewall.

Step 9: Run the MySQL Service as a Limited User. By default, the MySQL server service runs as a privileged local system user. MySQL can be run as a limited user to restrict its capabilities and limit what a compromised MySQL server is capable of.

Step 10: Encrypt the Data Folder. For users who store particularly sensitive information within MySQL, it is possible to encrypt the data directory of the MySQL installation. The encryption should be performed while the server is not running, and while the administrator is logged-in as the mysql user. Users should be aware that if the private key used to encrypt the data directory is lost, all data is lost. Performance will be diminished because all files must be decrypted before they can be accessed. Considering the risks of data and performance loss, data directory encryption is not recommended unless it is considered absolutely necessary, and then should only be used by experienced users.

Step 11: GRANT the Minimum Privileges Necessary. When creating new users and granting privileges, it is often easy to grant all privileges on a database or all privileges globally, but this should be avoided. When the administrator grants privileges, it should try to grant the minimum necessary for a user to perform only his assigned tasks.

Step 12: Change the Name of the Root User. The root user does not need to be named “root”. Most attackers will obviously try to compromise the “root” user account and will be stopped if there is no “root” user. Of course can be used any name, but the recommendation is not using your own name as administrator because an attacker might assume that an account with the administrator name would have root-level privileges.

CONCLUSIONS

When exiting home or automobile it’s become a natural reaction to take a moment to lock the doors and eventually to set the alarm. We do such things because we know that the possibility of items being stolen dramatically increases if we do not take such rudimentary yet effective precautions. In the IT industry at large the same things seems to happen.

The World Wide Web is a place where software evolution opens new doors to how the information can be presented to a user and how we do business. As these new opportunities become available, new ways to get at the sensitive data that is being stored in a database become available. These ways of acquiring sensitive data are changing daily and while new methods are implemented to protect this information, new ways to get around this protection are also being developed. In a production environment the database administrator needs to be aware of what the user is being allowed to do.

Note that malicious attacks aren’t the only cause of data damage or destruction. Far too many developers and administrators choose to work with accounts possessing privileges far exceeding what is required. Eventually a command is executed which never should have been permissible in the first place, resulting in serious damage. An uninvited database intrusion can wipe away months of work and erase inestimable value.

The topics covered above are just a few issues that a database administrator needs to take into consideration when he works with a database system. It’s strongly recommended for them to take adequate time to understand MySQL’s security features, because they should be making a regular appearance in all MySQL-driven applications.

REFERENCES

1. dev.mysql.com/doc/refman/5.0/en/ - MySQL 5.0 Reference Manual, Document generated on: 2007-11-23 (revision: 8847);
2. W. Jason Gilmore – Beginning PHP and MySQL from novice to professional, Fourth Edition, 2010;
3. http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf - The Imperva Application Defense Center (ADC) – White Paper: Consumer Password Worst Practices;
4. http://www.yassl.com/yaSSL/News/Entries/2011/4/27_Securing_MySQL_with_a_Focus_on_SSL.html - O'Reilly MySQL conference and Expo 04/12/2011, Chris Conlon, Security and Database Administration;
5. http://us3.php.net/manual/en/security.database.php - PHP online reference manual 01/10/2011, Database Security;
6. http://www.mysql.com/why-mysql/white-papers/sco-inside50.php - Inside MySQL 5.0 a DBA's perspective – A MySQL Business White Paper, 10/2005.

ALPHABETICAL INDEX OF AUTHORS